



CyberAI 4 Zero Trust Network Access

1 message

easytech4all tech <et4all.research@gmail.com>
Draft

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.

Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .

Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider Threat Detection (ITD) - Govt & Military etc.

BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict events 'days in advance' - Global Information

Dominance Experiments (GIDE) - AI + CLOUD

COMPUTING + SENSORS. Mix of military and civilian sensors to address scenarios where contested logistics might pose a problem. GIDE tech employs ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these weapons platforms can crash the software used to runthem. That could sideline a fighter jet or radar that protects a aircraft carrier battlegroup or cause a Military satellite to go offline using non kinetic means . Satellite navigation systems are also at risk of jamming and spoofing. Satellites are also crucial for coordinating electricity grids and time stamping financial transactions. Geolocation is susceptible to electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military industrial complex to take cyber vulnerabilities seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant

threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legitimate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials and additional authentication.

Such an attack has the opportunity to hit a massive quantity of targets but if reached to far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are vulnerable to Cyber Attack - Weapon Systems don't just include hypersonic missiles or lasers. There are computers at wings , at sea and on land. We don't think of weapons systems that way but none of them works without computers. These computers add functionality , including fire control (correcting and adjusting aim against distant or fast moving targets), navigation,(receiving AGPS signals) and communications (voice and data)

GLOBAL CYBER INTELLIGENCE – CONSECRATED

Global Cyber Intelligence Consecrated . This Video Presentation is rededicated to the International Cyber Defense Umbrella comprising of Military Alliance Cyber Commands , Government and Federal Cyber Defense Independent Cyber Threat Intelligence Analysts & Specialists.

KEY HIGHLIGHTS –

UN , US , NATO , INDIA , Federal Security Agencies , Military Cyber Force and Commands , Private CTI Agencies and Corporations.

Two invaluable book recommendations from UN and suggestions to UN . My recent reads .

"The Basic facts about UN" is a mini encyclopaedia . Not just about UN but Copernican World Events and Crisis/Conflict response at the Macro Level including the development and progress of ICT's and the ICT in outer space – Relevant Treaties and Agreements. UNISPACE conferences , cooperation with European Space Agency (ESA) , NASA , International Astronautical Federation (IAF) , Committee on Earth observation

The other Book uncommon opportunities – Agenda for Peace and Equitable development

The Report of the International Commission on Peace and Food by International Center for Peace and Development USA and M.S. Swaminathan Research Foundation Chennai India .

Highlights are the sections on the "Peace Imperative" – Information Superhighways, War as an instrument of Policy, Nuclear Weapons (START 1 , START 2 , NPT , CTBT , Ballistic Missiles) , Confidential Studies and what made it possible.

US Cyber Policy for Deterrence. Executive Order 14028 Improving the Nation's cybersecurity. This EO Mandates endpoint protection , defining logging requirements , implementing audit logging in a unified way and use ransomware to cripple critical infrastructure components related to National Security and the public . Enhancing existing information assurance security controls as a part of a Risk management framework

White House Cyber Physical Resilience Initiative (ISSA SIG) – Cyber Resilience refers to the ability to protect electronic data and systems from cyberattacks as well as to resume business operations quickly in case of resilience capabilities in each organisation. Yet cyber resilience is currently understood differently by various organisations despite the fact that NIST had published clear guidelines(800-160) then followed by others

NATO CCDCOE Locked Shields Livefire Exercise 2023 – a unique international Cyberdefence Exercise offering the most complex technical live fire challenge in the World. From a Strategic perspective the exercise covers various sectors and it's infrastructure. NATO Cyber Commanders Handbook 2.0 at stakeholders meeting in Tallinn Estonia – leveraging a cooperative approach for Cyber Defence.

India's meteoric rise in United Nations Specialised Agency for Information and Communication Technologies – International Telecommunication Union (ITU) ranking for everything Cybersec . Ranked at 10th from

USA and UK ranked First and Second respectively. Saudi Arabia and Estonia was ranked third. South Korea , Singapore , Spain shared the fourth spot . Russia , UAE , Malaysia shared the Fifth Spot . Lithuania came 6th . Also 3 Indian Leaders have been named in Global Hall of Fame report that identified "CLOUD SECURITY AS THE BIGGEST CHALLENGE" – Indian Govt once said that they want to make INDIA the Global hub for Cyber Ecosystem economy – Cybersecurity and Cyber Resiliency become of paramount importance mechanically.

Open Source Software is India's inherent Strength . A Quick analysis of the Internet and YouTube will reveal India's talent in Open Source OS Linux distros – Ubuntu , Fedora , Kali Linux , Elementary OS , Debian etc. have been developed and promoted further . The Beauty of OSS are the following.

Right to use study change distribute the software and its source code to anyone for any purpose.

Development in Collaborative Public Manner.

Examine the Code thereby facilitating public trust in the Software.

Linux has the largest installed base of all general purpose operating systems (including AOSP and ChromeOS) . From running the terminals at the International Space Station to some of the fastest supercomputers . The Chromebook, which runs the Linux kernel-based ChromeOS, dominates the US K-12 education market and represents nearly 20 percent of sub-\$300 notebook sales in the US. Linux is the leading operating system for supercomputers, and is the only OS used on TOP500 supercomputers (since November 2017, having gradually eliminated all competitors).

Linux also runs on embedded systems, i.e. devices whose operating system is typically built into the firmware and is highly tailored to the system. This includes routers, automation controls, smart home devices like Samsung, Hyundai, and Toyota all rely on Linux), spacecraft (Falcon 9's and Dragon 2's avionics use a customized version

More Snapshots in the above video presentation.

Future of the Intelligence Community Workforce – Enabling a Secure Hybrid Work Environment – CIA and MITRE Corp.

US Cert (Computer Emergency Response Teams) , Cybersecurity and Infrastructure Security Agency (CISA) National Security Agency (NSA) Events .

Intelligence and National Security Alliance (INSA) and ISSA (Information Systems Security Association) Brainstorms Webinars Seminars .

. EU Cyber Defence Innovation Program.

European Cyber Agora.

National Cyber Strategies to Defend Critical Infrastructure.

Global Annual Cybersecurity Summits and National Cybersecurity Alliance endeavours.

UKCSA UKSec – Challenges faced by Governments and International Law Enforcement.

. Cybersecurity Projections and Predictions.

Cyber Task Force – FBI Criminal Cyber Squad .

Cyber World Congress – 24 hr Virtual Events.

Cyber Threat Intelligence Talks.

. CyberAI and its impact on OSINT.

Cyber Intelligence Units Quarterly Updates (Infoblox)

CYBERWARFARE PREPAREDNESS by Allen Ari Dziwa.

Military Cyber Commands and Cyber Force (SoC- Trident Jaguar)

Assessing the risk and Protecting the Supply Chain.

. Podcast on Cyberweapons.

. Future of Cybersecurity and Risk Analysis.

Cyber Threat Intelligence and Incident Response.

Cybersecurity Advanced Persistent threat Defenders Overview.

. Virtual Intelligent Automation Exchange – Director of AI Defense Intelligence Agency (DIA)

. Small Business National Security Showcase (Directorate of Digital Innovation CIA)

. CISO perspective – Delta Airlines.

. Cyber Strategies for a World at War (Open Source Aggregation and Analysis).

. WEF and INTERPOLs Global Risk Annual Assessments and SOC – Cyber Ploygon.

Google Cloud Security talks and threat Analysis Group.

Digital Risk Management e-learning platform for mediators. UN DPPA and Cyberpeace Institute.

1PowerCyber @ Easytech4all CTI Research & Analysis consultancy focuses it's energies on Military Cyber Commands and Global Federal Agencies CTI reports , webinars , brainstorm , bright talks by global intel experts , infographics and video content presentations to be used for Blogs , Digital Magazines , Newsletters and CMS .

This Knowledge pool also facilitates analysis and benchmarking of EDR/NDR , SIEM , SOAR solutions available for different ecosystems . This coupled with OSINT research conducted through different search engines . Eventually this threat intel gets included on Collaborative CMS & services integration platform.

Cyber Strategic Communication based on OSINT and Global Cyber Policy Analysis also remains an area of Major interest as it is indispensable for future Cyber threat projections.

OS Hardening – Mapping Desktop / Mobile OS and Application Security with every successive firmware and security patch is continuous work in progress at the Threat Intel Research Consultancy.

This Video Presentation is a succinct snapshot of some Preliminary and detailed experience with Global Cyber Intelligence Think Tanks , Organizations and Associations .

From Researching Analysing Cybersecurity and CTI Products/Services to functioning as a Cyber Threat Intel Provider for Governments , Global Agencies and CTI Organisations. The Scope for Transnational Cyber Threat Intelligence.

1Power Easytech4all Cyber threat Intelligence Solution primarily relies on the Cyber Prudence and Strategic Insights of Global Experts from UN Cyber Policy Assessments and Debates on ICT's , White House Cyber Strategy , UNIDIR , European Defence Agency (EDA) , National Security Agency (NSA) , Cybersecurity and Infrastructure Security Agency (CISA) , Federal Bureau of Investigation (FBI) , World Economic Forums (WEF) Annual Global Risks Report .

They are the Cyber beacons for the World shaping Global Cyber Policy and Cyber Deterrence Countermeasures plus standards .

1PowerCyber @ easytech4all.net

<https://1powercyber.substack.com>

<https://1powercyber.blogspot.com>

<https://easytech4all.tumblr.com>

<https://linktr.ee/1powercyber>

The policy challenges presented by cyberspace are not solely technological in nature. The cyber domain is a human-made environment and is fundamentally shaped by human behaviour. It amplifies such behaviours for better or worse, the impacts of which are usually also felt in the physical world. Cyberspace is owned and operated by private companies, governments, non-profit organisations, individual citizens and even criminals. This means that any strategic response to this context must link geostrategy and national security, criminal justice and civil regulation, economic and industrial policy and requires a deep understanding of the different cultural or social contexts and value systems interacting online.

Cyberspace also transcends national borders. Technology supply chains and critical dependencies are increasingly global, cyber criminals and state-based actors operate from around the world, powerful technology companies export products and set their standards, and the rules and norms governing cyberspace and the internet are decided in international fora. Cyberspace is also continually evolving as technology and the ways people use it change, requiring us to adopt an agile and responsive approach.

What is cyberspace?

To many of us, cyberspace is the virtual world we experience when we go online to communicate, work and conduct everyday tasks. In technical terms, cyberspace is the interdependent network of information technology that includes the internet, telecommunications networks, computer systems and internet-connected devices. For the military,

and when considering our efforts to counter threats in cyberspace, it is an operational domain, along with land, sea, air and space.

How is cyberspace experienced?

Cyberspace is, by definition, a 'shared' space and its scale and complexity means that every person's experience of it is unique. Citizens access cyberspace when they check their bank accounts online or stream a film at home. Businesses use cyberspace to connect their staff with the resources they need, whether this is access to information or control over a manufacturing process. Governments provide public services to their citizens using online portals. Cyber professionals look 'under the hood' at the technology, standards and protocols that make it all 'just work' for users. All these groups use cyberspace in different ways and for different purposes, and we are all making an ever-greater use of it.

Cyberspace can be described in terms of three layers:

Virtual

The part of cyberspace most people experience. It consists of representations of people and organisations through a virtual identity in a shared virtual space. Virtual representations could be an email address, user identification, a social media account or an alias. One person or one organisation can have multiple identities online. Conversely, multiple people or organisations could also create just a single, shared identity.

Logical

The part of cyberspace made up of code or data, such as operating systems, protocols, applications and other software. The logical layer cannot function without the physical layer and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer, allows virtual identities to communicate and act.

Physical

The physical layer of cyberspace includes all the hardware on which data is transmitted, from the routers, wires and hubs that you have in your home, to large complex telecommunications systems operated by big tech companies. As well as physical infrastructure it includes the electromagnetic spectrum on which data is transmitted, such as WiFi and radio.

Cyber attacks can have devastating consequences for both companies and their customers. Network compromise can lead to unauthorized access to and theft of both business and customer data. In 2022 in the

Manage cyber security risk

In order to manage cyber security risk, government organisations must be able to identify, assess and understand them. The foundation of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them – whether internal to an organisation or emanating from its supply chain. Clear accountability and robust assurance will ensure that risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately.

Information about vulnerabilities must be shared across governments to provide a central view of critical vulnerabilities that will enable cross-government risks to be identified and managed, facilitating rapid assessment, coordination and mitigation at scale.

Protect against cyber attack

The protective stance of individual government organisations will be inextricably linked to their assessment and management of risk. While it will never be possible to protect against all attacks, those accountable must be able to demonstrate that they have appropriately considered those risks and responded accordingly.

Proportionate cyber security measures must be embedded in the technology government uses, and technology and digital services will be correctly designed, configured and managed. Crucially, governments must develop its shared capabilities, tools and services to address common cyber security issues at scale, improving cyber security across the whole of government as well as driving efficiency and value for money.

3. At the heart of any government's responsibility must be to protect the data it handles. As well as appropriately classifying information, governments must handle and share it in a way that is commensurate with the risks it presents, using the appropriate IT Systems.

Detect cyber security events

Building on the foundation of risk management and commensurate protective measures, governments must develop its capability to detect cyber security events across every part of its estate to ensure that risks can be mitigated before they critically impact government functions and services.

This means having the capability to monitor systems, networks and services to detect cyber security events before they become incidents. Enhanced coordination will enable governments to have the agility to use these data inputs to detect at pace and scale, facilitating coherent responses as well as providing the capabilities to detect more sophisticated attacks.

Minimise the impact of cyber security incidents

While effective risk management, appropriate and proportionate protective measures and enhanced detection capability will make governments a considerably hardened target, government organisations will still be impacted by cyber security incidents.

Governments must therefore be fully prepared and able to respond to cyber incidents with the capability to restore affected systems and assets and resume the operation of its functions and services with minimal disruption. A critical component of this will be establishing the mechanisms to test and exercise incident response plans, both organisationally and across government, as well as the ability to learn lessons from incidents and 'near misses'.

Cyber Critical Infrastructure | Nuclear impingement

CCI | Nuclear Reimagined

CCI Infra – Nuclear Landscape | NCAM 2022

Role of Dynamic Multidimensional Security Approach Zero Trust Network Access on Critical Infrastructure.

Cyber Attacks on Critical Infrastructure | NATO

Zero Trust Architected Networks – US Cybersecurity and Infrastructure Security Agency . Department of Homeland Security

US Intelligence and National Security Alliance

Protecting Critical Infrastructure: Key Elements of the New National Cybersecurity Strategy

Tuesday, May 2 | 1:00 – 2:30 PM ET | Virtual – two-part program!

Panelists:

Brian Scott, Deputy Assistant National Cyber Director for Cyber Policy and Programs, Office of the National Cyber Director, Executive Office of the President

Speaker from CISA (Invited)

Chris Boyer, Executive Committee Member, Communications Sector Coordinating Council, and VP, Global Security and Technology Policy, AT&T

Amanda Craig, Executive Committee Member, IT Sector Coordinating Council and Senior Director, Global Cybersecurity Policy, Microsoft

Matthew Eggers, VP for Cybersecurity Policy, U.S. Chamber of Commerce

<https://insaonline.us8.list-manage.com/track/click?u=2bbe7114be6cc1ae543a8f374&id=4f659e75a0&e=d386303ff8>

Cyber Council – New White Paper

Industry Contributions to Offensive Cyber Operations, outlines the importance of public/private collaboration in cybersecurity and provides five key recommendations that can help strengthen U.S. critical infrastructure

<https://insaonline.us8.list-manage.com/track/click?u=2bbe7114be6cc1ae543a8f374&id=aa1dc2fed6&e=d386303ff8>

Key Highlights of Google Cloud Security – 2023 Outlook

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-1>

Frontline Threat Intel Panel

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-2>

Cyber Crime Metamorphosis: A Case Study Examining How Criminals Adapt to Chaos

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-3>

Managing Open Source Software Security

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-4>

DDoS Trends at US Elections and What's New with Cloud Armor

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-5>

Defeating Cryptomining Attacks with Native Security Controls

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-6>

Cloud Detection & Response Survey: Challenges and Insights

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-7>

Office of the CISO
RESOURCES

Improve Decision Making with Automated Contextual Awareness

<https://cloudonair.withgoogle.com/events/2023-emea-security-talks?talk=na-talk-8>

Quick recap of Global Cyber Threat Intelligence brainstorms (2019-2022) by <https://1Power.substack.com> and <https://easytech4all.net>

US Federal Agencies. Security Organisations

US Cyber Command.NSA.US Dept of Homeland Security.Department of Defense . Secret Service CID. CISA.FBI

https://1powercyber.blogspot.com/2022/05/us-cybersecurity-global-conference.html?utm_source=pocket_mylist

UN Security Council Cyber Threats Debate –

UNIDIR Cyber Stability Conference 2021 & AI Disruption Peace Security (innovations dialogue) 2022

<https://1powercyber.substack.com/p/unidir-cyber-stability-conference>

Importance of Information and Communication technologies .

NATO Locked Shields 2022

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

Cyber Polygon with World Economic Forum and INTERPOL

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega?utm_source=pocket_mylist

White House National Cybersecurity Strategy

<https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html>

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

Ransomware Attackers Defenders – FBI's perspective

US Cyberspace Solarium Commission

UK Cybersecurity Association with Digital Police Center.

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

Fourth CEO Summit – USA

State of American Business 2023

Challenges faced by Government and international LAW Enforcement

Intelligence and National Security Alliance (INSA) 2022 UPDATE

What is Advanced Cyber Threat Intelligence ?

Accreditations Webinars LMS – Cybersec CTI

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

<https://1powercyber.substack.com/p/google-cloud-security-summit-with>

Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM) software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. The term and the initialism SIEM was coined by Mark Nicolett

https://1powercyber.substack.com/p/security-information-and-event-management?utm_source=pocket_mylist

Zero Trust Architected Networks by Cybersecurity and Infrastructure Security Agency

1PowerCyber and Easytech4all Global CTI Research & Analysis.

Mapping Global CTI Landscape and Visual Trends

International Cyber Threat Intelligence Brainstorms

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

Global Cyber Threat Landscape

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

https://1powercyber.substack.com/p/cyber-kinetic-warfare?utm_source=pocket_mylist

Cyber Independence and Freedom

Cyberattacks and Critical Infrastructure (Reading & Resources)

Space Threats and Satellite Navigation Systems

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for [Easytech4all.net](https://easytech4all.net)

<https://bit.ly/3P8gCTT>

Advanced Cyber Threat Intelligence Research Analysis Assessment and Projections . Video Playlist .

<https://bit.ly/3yqDEje>

Advanced Cyber Defense Threat Intelligence Blog in Progress

<https://easytech4all.net/author/easytechonline/>

<https://1powercyber.substack.com>

<https://1powercyber.blogspot.com>

<https://easytech4all.tumblr.com/>

References

Clarke R.A, K. R. (2010). Cyber war: the next threat to national. eCCO.

Clarke, R. (2011). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.

Cybersecurity and Infrastructure Agency. (2021, October 15). CISA HOME. Retrieved October 14, 2021, from <https://www.cisa.gov/about-cisa>

Gazula, M. B. (2017). Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology .

Jeremy Rabkin, A. R. (2016). Hacking Back Without Cracking Up. Aegis Paper Series No. 1606.

Kukuh Ugie Sembodho, A. T. (2021). The Limitation of United States Deterrence Strategy Towards North Korean Cyber . Global Strategis, p. 150.

Libicki, M. (2009). Cyberdeterrence and cyberwar. Santa Monica: The Rand Corporation.

M, T. (2012). An analysis for a just cyber warfare in Cyber Conflict (CY-CON). , 2012 4th International Conference on, (pp. 1-10).

National Security Agency. (2021, October

14). NSA Home.

Parks R, D. D. (2011). Principles of cyberwarfare, security privacy. IEEE, 30-35.

Rid, T. (2012, March). Think Again: Cyberwar. Foreign Policy , pp. 80-84.

Sanger, D. (n.d.). The Perfect Weapon: War, Sabatoge, and Fear in the Cyber Age. New York: Crown Publishers.

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review, [269-270](#).

Tallin Mannual. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

The White House. (2011, April). National Strategy for Trusted Identities in

Cyberspace.

The White House. (2021). Improving the Nation's Cybersecurity. Federal Register Vol. 86.

Trautman, L. J. (2016, April). Cybersecurity: What About US Policy? Journal of Law, Technology & Policy, p. 344.

US Cyber Command. (2021). US Cyber Command Mission. Retrieved from <https://www.cybercom.mil/About/Mission-and-Vision/>

The dramatic surge in open source software supply chain attacks has sent defenders scrambling to find mitigations and solutions.

Software supply chain attacks increased by 742% at a time when we depend on open source software to build 97% of all enterprise code.

Security debt is a real problem for most organizations in the world today and the attackers will utilize this to their advantage. The more vulnerabilities a company has, the more likely it is that a malicious actor will exploit them and a data breach soars.

To prevent security debt from building up, defenders must keep system hygiene front of mind and focus on proper network zone segmentation, essentially building a zero-trust networks.

Distributed denial of service attacks, or DDoS attacks, see malicious actors attempt to disrupt a site by overwhelming its infrastructure with a large amount of internet traffic. As DDoS attacks overwhelm a site's

Cloudflare Blocks Record DDoS Attack as Threats Surge

The attacks, which originated from more than 30,000 different IP addresses, targeted websites including a gaming provider, cryptocurrency companies, hosting providers, and cloud computing platforms

In today's interconnected world, critical infrastructure is under constant threat from cyberattacks that can compromise the availability, integrity, and confidentiality of essential systems and services. As a result, g

With a predicted 25.4 billion active Internet of Things (IoT) devices worldwide in 2030, companies should be looking to protect it as a rapidly growing asset and target for cyber attacks.

Research by Nozomi Networks Labs for its OT/IoT security report has found that in the latter half of 2022, IoT devices were frequently targeted by malicious actors aiming to gain control of them. Likewise, Opera

The ever-present threats of ransomware and data breaches make it imperative to lock down systems and prevent attackers from gaining a foothold. Hardening a system means reducing its attack surface and in

The Domain Name System (DNS) is one of the oldest internet infrastructures, and often overlooked in security. However, through it passes an incredible amount of attack traffic. Attackers often use DNS to cond

State of the Internet (SOTI) report to gain insights into malicious DNS traffic and its potential impact: By Akamai.

26% of infected devices have reached out to identified initial access broker (IAB) C2 domains, including Emotet- and QakBot-related domains.

IABs present a large risk to organizations, as their primary role is to do the initial breach and sell access to ransomware groups and other cybercriminal groups.

30% of affected organizations are in the manufacturing sector — twice as many as the second-largest vertical.

Network-attached storage (NAS) devices are ripe for exploitation, as they are less likely to be patched and hold troves of valuable data. Our data shows attackers are abusing these devices through QSnatch.

Malware is a fast-growing, ever-evolving threat to cyber security. In the first six months of 2022, over 2.8 billion malware attacks were reported worldwide. Beyond risks to their network, malware like ransomware has a global cost of ransomware in 2015, which was \$325mn.

CLOUD SECURITY.

"Cybersecurity remains at the top of every organisation's agenda. Google Cloud's unique capabilities and expertise can help organisations, large and small, in the public or private sector, address today's most pro

* Zero Trust

* Securing the Software Supply Chain

* Ransomware and other emerging threats

* Cloud governance and Digital Sovereignty

Whether you use our trusted cloud for digital transformation, or continue to operate on-premise or in other clouds, you'll learn how we can help you be safer with Google."

<https://cloudonair.withgoogle.com/events/summit-emea-security-2022#:~:text=Cybersecurity%20remains%20at,safer%20with%20Google>.

Complete End to End Cyber Threat Intelligence Solution - Virustotal + Chronicle + Siemplify

The U.S. government has improved its alert process for emerging cyberthreats to the United States and its allies and partners around the world—with the U.S. Computer Emergency Response Team (US-CERT) alerting adversaries tactics, techniques, and procedures (TTPs).

Describing adversary behavior using the CTI knowledge base is a cornerstone of the threat-informed defense paradigm. Techniques rarely occur in isolation, and instead, the attacker typically uses each technique

Emotet continues to be used in wide broad-based attacks against victims in all sectors across the world.

The infamous botnet has been disrupted thanks to an international effort across the US, Canada, and several European nations.

Quick recap of Global Cyber Threat Intelligence brainstorms (2019-2022) by <https://1Power.substack.com> and <https://easytech4all.net>

US Federal Agencies. Security Organisations

US Cyber Command.NSA.US Dept of Homeland Security.Department of Defense . Secret Service CID. CISA.FBI

<https://easytech4all.net/cyber-conference/>

https://1powercyber.blogspot.com/2022/05/us-cybersecurity-global-conference.html?utm_source=pocket_mylist

UN Security Council Cyber Threats Debate -

<https://easytech4all.net/2022/03/06/un-security-council-cyberthreats-debate/>

UNIDIR Cyber Stability Conference 2021 & AI Disruption Peace Security (innovations dialogue) 2022

<https://easytech4all.net/2022/07/05/unidir-cyber-stability-conference-3rd-december-friday-2021/>

<https://1powercyber.substack.com/p/unidir-cyber-stability-conference>

Importance of Information and Communication technologies .

<https://easytech4all.net/2022/02/05/unidir-ict-information-communication-technologies/>

NATO Locked Shields 2022

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

Cyber Polygon with World Economic Forum and INTERPOL

<https://easytech4all.net/2022/01/16/cyber-polygon-2020-2021-and-2022/>

https://1powercyber.substack.com/p/wef-and-interpol-cybersecurity-mega?utm_source=pocket_mylist

White House National Cybersecurity Strategy

<https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html>

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

<https://easytech4all.net/2021/05/09/nownext-countering-ransomware-attacks/>

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

<https://easytech4all.net/cyber-essentials-us-dhs/>

Ransomware Attackers Defenders - FBI's perspective

<https://easytech4all.net/ransomware-attackers-defenders-fbis-perspective/>

US Cyberspace Solarium Commission

<https://easytech4all.net/2022/04/10/us-cyberspace-solarium-commission/>

UK Cybersecurity Association with Digital Police Center.

<https://easytech4all.net/uk-cybersecurity-association-1-day-summit/>

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

<https://easytech4all.net/2022/02/07/4th-annual-national-cybersecurity-summit-by-cisa/>

Fourth CEO Summit - USA

<https://easytech4all.net/2022/06/27/iv-ceo-summit-of-the-americas/>

State of American Business 2023

https://easytech4all.net/state-of-american-business-2023/?utm_source=pocket_mylist

Challenges faced by Government and international LAW Enforcement

<https://easytech4all.net/2021/10/06/watch-challenges-faced-by-govt-and-int-law-enforcement-cybersec-on-youtube/>

Intelligence and National Security Alliance (INSA) 2022 UPDATE

<https://easytech4all.net/future-of-intelligence-community-workforce/>

What is Advanced Cyber Threat Intelligence ?

<https://easytech4all.net/2020/09/20/what-is-advanced-cyber-threat-intelligence/>

Accreditations Webinars LMS - Cybersec CTI

<https://easytech4all.net/2020/12/29/cybersec-accreditation-nanocertifications/>

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

<https://1powercyber.substack.com/p/google-cloud-security-summit-with>

Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM) software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. The term and the initialism SIEM was coined by Mark Nicolett

https://1powercyber.substack.com/p/security-information-and-event-management?utm_source=pocket_mylist

Zero Trust Architected Networks by Cybersecurity and Infrastructure Security Agency

<https://easytech4all.net/2021/10/10/zero-trust-architected-networks-advanced-cyber-threat-intelligence/>

1PowerCyber and Easytech4all Global CTI Research & Analysis.

<https://easytech4all.net/internet-ranking-advanced-cyber-threat-intelligence/>

<https://easytech4all.net/2021/02/21/easytech4all-ranking-for-advanced-cyber-threat-intelligence/>

<https://easytech4all.net/2020/12/30/3452-best-cybersecurity-stories-by-easytech4all-on-flipboard-quick-updates/>

<https://easytech4all.net/2021/02/14/mapping-global-ranking-for-advanced-cyber-threat-intelligence/>

International Cyber Threat Intelligence Brainstorms

<https://easytech4all.net/1-power-cybersec-cti-brainstorms/>

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

<https://easytech4all.net/2022/04/10/safe-and-secure-digital-ecosystems-for-students/>

Global Cyber Threat Landscape

<https://easytech4all.net/cyber-threat-intelligence-landscape/>

<https://easytech4all.net/cyberwar-ww3-flashpoint/>

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

https://1powercyber.substack.com/p/cyber-kinetic-warfare?utm_source=pocket_mylist

Cyber Independence and Freedom

<https://easytech4all.net/2021/08/14/cyber-independence-freedom/>

Cyberattacks and Critical Infrastructure (Reading & Resources)

<https://easytech4all.net/2021/10/01/cyberattacks-critical-infrastructure-nato/>

Space Threats and Satellite Navigation Systems

<https://easytech4all.net/2022/03/06/threats-to-satellite-navigation-system-conflict-in-space/>

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for [Easytech4all.net](https://easytech4all.net)

<https://bit.ly/3P8gCTT>

Advanced Cyber Threat Intelligence Research Analysis Assessment and Projections . Video Playlist .

<https://bit.ly/3yqDEje>

Advanced Cyber Defense Threat Intelligence Blog in Progress

<https://easytech4all.net/author/easytechonline/>

<https://1powercyber.substack.com>

<https://1powercyber.blogspot.com>

<https://easytech4all.tumblr.com/>

<https://medium.com/@1PowerCyber>

References

Clarke R.A, K. R. (2010). Cyber war: the next threat to national. eCCO.

Clarke, R. (2011). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins.

Cybersecurity and Infrastructure Agency. (2021, October 15). CISA HOME. Retrieved October 14, 2021, from <https://www.cisa.gov/about-cisa>

Gazula, M. B. (2017). Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology .

Jeremy Rabkin, A. R. (2016). Hacking Back Without Cracking Up. Aegis Paper Series No. 1606.

Kukuh Ugie Sembodho, A. T. (2021). The Limitation of United States Deterrence Strategy Towards North Korean Cyber . Global Strategis, p. 150.

Libicki, M. (2009). Cyberdeterrence and cyberwar. Santa Monica: The Rand Corporation.

M, T. (2012). An analysis for a just cyber warfare in Cyber Conflict (CY-CON). , 2012 4th International Conference on,, (pp. 1-10).

National Security Agency. (2021, October

14). NSA Home.

Parks R, D. D. (2011). Principles of cyberwarfare, security privacy. IEEE, 30-35.

Rid, T. (2012, March). Think Again: Cyberwar. Foreign Policy , pp. 80-84.

Sanger, D. (n.d.). The Perfect Weapon: War, Sabatoge, and Fear in the Cyber Age. New York: Crown Publishers.

Schmitt, M. (2014). The Law of Cyber Warfare: Quo Vadis? Stanford Law & Policy Review, 269-270.

Tallin Mannual. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

The White House. (2011, April). National Strategy for Trusted Identities in

Cyberspace.

The White House. (2021). Improving the Nation's Cyber

security. Federal Register Vol. 86.

Trautman, L. J. (2016, April). Cybersecurity: What About US Policy? Journal of Law, Technology & Policy, p. 344.

US Cyber Command. (2021). US Cyber Command Mission. Retrieved from <https://www.cybercom.mil/About/Mission-and-Vision/>

How the threat landscape has changed over time with the advent of AI

AI impact on cybersecurity -

AI Cyberdefense systems are being implemented to proactively detect and mitigate threats. Traditional antivirus relies on blacklisting historic threats based

on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -

EDR - USER AUTHENTICATION - NETWORK DETECTION - INTRUSION

DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent. AI based biometric surveillance systems are increasingly being used in sensitive contexts without individuals knowledge or consent.

Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

AI for cybersecurity and cybersecurity for AI.

AI in cybersecurity presents great opportunities but as with any powerful general purpose dual use technology , it also brings great challenges. AI can

improve cybersec and defence measures allowing for greater system robustness , resilience and responsiveness but AI in the form of ML and deep learning will escalate sophisticated cyberattacks enabling faster. The application of AI in cybersecurity also poses security and ethical concerns.

Among other things it remains unclear to see how responsibilities for autonomous response systems should be ascribed. How to make sure systems

are behaving according to expectations. Or what the security risks carried by the increasing anthropomorphisation of AI systems are. ANTHROPOMORPHIC LANGUAGE AT TIMES APPEARS INTRINSIC TO THE FIELD

The Organisation for economic cooperation and development (OECD) defines an AI system as

a "machine based system that can for a given set of human defined objectives make predictions recommendations or decisions influencing real or virtual environments." This definition has also been accepted and

ML is a set of techniques to allow machines to learn in an automated manner through patterns and inferences rather than through explicit instructions through a human. ML approaches often teach machines to learn by trial and error.

Neural networks involve repeatedly interconnecting thousands or millions of simple transformations into a larger statistical machine that can learn sophisticated relationships between inputs and outputs. Neural networks create links between inputs and outputs .

Deep learning is a large neural network subset composed of hierarchical layers that increase the complexity of the relationships between input and output.

AI in cybersecurity can be identified in 3 categories. - Detection 51% Prediction 34% and response 18%.

Driving forces that are boosting the use of AI in cybersecurity.

1. Speed of impact – in some of the major attacks the average time of impact on the organisation is 4 mins.

Today's attacks are not just ransomware or just targeting certain systems or vulnerabilities they can move and adjust based on what the targets are doing. These kind of attacks impact incredibly quickly and they

2. Operational complexity. - Today the proliferation of cloud computing platforms and the fact that those platforms can be operationalised and deliver services quickly in the milliseconds range. Means that you cannot have a lot of humans in that loop and you have to think about a more analytics driven capability.

3. Skills gap – There is a global shortage of about a million and a half cybersecurity professionals. This level of scarcity pushes the industry to automate at a faster rate.

AI can help security teams in 3 ways. - By improving systems robustness response and resilience ...The 3R model.

AI can improve systems robustness that is the ability of a system to maintain its initial assumed stable configuration even when it processes erroneous inputs. Thanks to self testing and self healing software. The 3R

AI can strengthen systems resilience – the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.

AI can be used to enhance response – the capacity of a system to respond autonomously to attacks , to identify vulnerabilities in other machines and to operate strategically by deciding which vulnerability to attack

Identifying when to delegate decision making and response actions to AI and the need of an

individual org to perform risk impact assessment are related. In many cases AI will augment

without replacing the decision making of human security analysts and will be integrated into

the process that accelerate response times.

AI Cyberdefense systems are being implemented to proactively detect and mitigate threats. Traditional antivirus relies on blacklisting historic threats based on virus signatures. AI based EDR can recognise aspe

MAJOR APPLICATION IN -

EDR - USER AUTHENTICATION - NETWORK DETECTION - INTRUSION

DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.

Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify

patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .

Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human

behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider

Threat Detection (ITD) - Govt & Military etc.

BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber

threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict

events 'days in advance' - Global Information

Dominance Experiments (GIDE) - AI + CLOUD

COMPUTING + SENSORS. Mix of military and civilian

sensors to address scenarios where contested

logistics might pose a problem. GIDE tech employs

ML based system to send fast critical updates and

alerts. Can prevent surprise aggression or lead to

negotiations instead of conflict . Humans will still be

heavily involved in the process.

Complex weapons platforms also coordinate

attack or defense among geographically

disparate forces. A CyberAttack on these

weapons platforms can crash the software

used to run them. That could sideline a

fighter jet or radar that protects a aircraft

carrier battlegroup or cause a Military

satellite to go offline using non kinetic

means - Lasers , radio frequency jammers and Cyberattacks . Satellite navigation systems are also

at risk of jamming and spoofing. Satellites

are also crucial for coordinating electricity

grids and time stamping financial

transactions. Geolocation is susceptible to

electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military indu

seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of

contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant

threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legitimate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials

Such an attack has the opportunity to hit a massive quantity of targets but if reached too far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are

vulnerable to Cyber Attack - Weapon Systems don't

just include hypersonic missiles or lasers. There are

computers at wings , at sea and on land. We don't

think of weapons systems that way but none of them

works without computers. These computers add

functionality , including fire control (correcting and

adjusting aim against distant or fast moving

targets), navigation,(receiving AGPS signals) and

communications (voice and data)

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent. AI based biometric surveillance systems are increasingly being used in sensitive contexts without individuals knowledge or consent.

Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including

strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

Cyber Intelligent Attacks .

1. AI driven Malware - Artificially intelligent malware can infect devices faster than ever before becoming harder to detect targeting more victims and creating more convincing phishing attacks.

2. Vulnerable Applications - Weak application security creates an entry point for APT to infiltrate computer systems. AI can be used to hide malicious code within applications , sometimes programming the attack worth a thousand lines of malware. Malware hidden in images developed by AI can only be detected by AI.

3. Expanded attack surface - Hybrid work and cloud access in personal devices widens the surface area for cyberattacks. AI creates an even more involved landscape expanding what devices and machines can

4. Constant evolution - AI is always evolving. While the benefits include enhanced threat detection. APT are constantly learning from advanced AI tools to develop more advanced attacks and improve their malware.

Therefore it's about time to intelligently automate endpoint security , email security , Application security , identity and access management.

Thanks to

1. NORTH ATLANTIC TREATY ORGANISATION.

2. UN APPOINTED INDEPENDENT RIGHTS EXPERTS.

3. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.

4. NATIONAL SECURITY AGENCY.

5. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

6. INFORMATION SYSTEMS AND SECURITY ASSOCIATION I

NTERNATIONAL.

7. EUROPEAN DEFENCE AGENCY.

8. EUROPEAN PARLIAMENTARY RESEARCH SERVICE.

1PowerCyber @ easytech4all.net

<https://1powercyber.substack.com>

<https://1powercyber.blogspot.com>

<https://easytech4all.tumblr.com>

<https://linktr.ee/1powercyber>

CyberAI Analysis.

<https://easytech4all.net/2023/08/30/advanced-cyber-threat-intelligence-document-presentation/>

<https://easytech4all.net/2023/08/30/my-qa-sessions-with-google-bard-large-language-model-a-little-organised-readers-discretion-advised/>

<https://easytech4all.net/2023/08/28/some-interactions-with-openai-chatgpt4-on-ai-and-relevant-domains-readers-discretion-advised/>

<https://easytech4all.net/2023/08/28/rendezvous-with-googles-bard-beta/>

<https://easytech4all.net/2023/09/11/7th-annual-defense-news-conference/>

<https://1powercyber.substack.com/p/advanced-cyber-threat-intelligence>

<https://1powercyber.substack.com/p/global-cyber-intelligence-research>

<https://1powercyber.substack.com/p/cyber-threat-intelligence-reflections>

Global Cyber Defense Threat Intelligence Observations.

<https://easytech4all.net/2023/03/21/quick-global-cyber-threat-intelligence-observations-22-23/>

<https://1powercyber.substack.com/p/cyberais-impact-on-cybersecurity>

<https://1powercyber.substack.com/p/the-evolving-cyber-landscape>

Global Cyber Intelligence - Consecrated

<https://easytech4all.net/2023/06/07/global-cyber-intelligence-consecrated/>

CyberAI - Inter Continental Strategic Imperative.

<https://1powercyber.blogspot.com/2023/06/ai-for-cybersecurity-and-cybersecurity.html?m=1>

NATO - Strategic Competition in Cyberspace

<https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html>

Google Cloud Security Conference 2023

<https://easytech4all.net/2023/06/07/google-cloud-security-2023/>

NATO Locked Shields

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

UNIDIR Cyber Stability Conference

<https://easytech4all.net/2023/04/02/unidir-cyber-stability-conference-2023/>

Blog for work in progress updates on R&A

<https://easytech4all.net>

<https://easytech4all.net/author/easytechonline/>

White House National Cybersecurity Strategy

<https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html>

Countering Ransomware with Department of Homeland Security , Cybersecurity and Infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

<https://easytech4all.net/2021/05/09/nownext-countering-ransomware-attacks/>

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

<https://easytech4all.net/cyber-essentials-us-dhs/>

Ransomware Attackers Defenders - FBI's perspective

<https://easytech4all.net/ransomware-attackers-defenders-fbis-perspective/>

US Cyberspace Solarium Commission

<https://easytech4all.net/2022/04/10/us-cyberspace-solarium-commission/>

UK Cybersecurity Association with Digital Police Center.

<https://easytech4all.net/uk-cybersecurity-association-1-day-summit/>

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

<https://easytech4all.net/2022/02/07/4th-annual-national-cybersecurity-summit-by-cisa/>

Challenges faced by Government and international LAW Enforcement

<https://easytech4all.net/2021/10/06/watch-challenges-faced-by-govt-and-int-law-enforcement-cybersec-on-youtube/>

Intelligence and National Security Alliance (INSA) 2022 UPDATE

<https://easytech4all.net/future-of-intelligence-community-workforce/>

What is Advanced Cyber Threat Intelligence ?

<https://easytech4all.net/2020/09/20/what-is-advanced-cyber-threat-intelligence/>

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

<https://1powercyber.substack.com/p/google-cloud-security-summit-with>

CyberKinetic and 5G

https://1powercyber.blogspot.com/2022/05/cyber-kinetic-world-war-3-and-5g-in.html?utm_source=pocket_mylist

Cyberattacks and Critical Infrastructure (Reading & Resources)

<https://easytech4all.net/2021/10/01/cyberattacks-critical-infrastructure-nato/>

Space Threats and Satellite Navigation Systems

<https://easytech4all.net/2022/03/06/threats-to-satellite-navigation-system-conflict-in-space/>

https://1powercyber.substack.com/p/space-threats-satellite-navigation?utm_source=pocket_mylist

Comsec Protocols and Paradigms

https://1powercyber.substack.com/p/comsec-protocols-and-paradigms?utm_source=pocket_mylist

Mapping Global CTI Landscape and Visual Trends

<https://easytech4all.net/2021/02/14/mapping-global-ranking-for-advanced-cyber-threat-intelligence/>

International Cyber Threat Intelligence Brainstorms

<https://easytech4all.net/1-power-cybersec-cti-brainstorms/>

Safe and Secure Digital Ecosystem for Schools by US Department of Homeland Security and Department of Justice

<https://easytech4all.net/2022/04/10/safe-and-secure-digital-ecosystems-for-students/>

Advanced Cyber Threat Intelligence Landscape and Updates via Digital Magazine by 1PowerCyber for [Easytech4all.net](https://easytech4all.net)

<https://bit.ly/3P8gCTT>

1 CyberAI and its impact ?

What types of AI are poised for the most growth in 2021 , 2022 and 2023 ?

Why are self-service and predictive analytics growing so much?

How are companies using AI, and specifically virtual assistants, functionally?

Which AI platforms and analytics tools are companies using the most?

What kind of success metrics are they seeing, in areas such as revenue increase, cost decrease, and customer ratings?

2 Cybersec in Fintech

Despite pouring billions of dollars into security, financial institutions continue to be the number one target of cybercriminals.

The digital transformation undertaken by this industry is contributing to this challenge as it has opened new doors for attackers, making customer data management and protection increasingly difficult.

The huge amount of financial transactions generated by retail organisations poses an attractive target for threat adversaries. While the predominant threat to the retail industry has traditionally been from criminal ransomware attacks affecting retailers.

3 Cyber Threat Intelligence -Brief Analysis

True threat intelligence involves collaboration with peers in industry, cross industry, with law enforcement and with regulatory bodies. It is understood that to call it "intelligence," TI has to be a public/private com

Fundamentally, organizations must be able to leverage their cyber security to protect everything. From firewalls and devices (whether at the edge or on-site), to data stored in the cloud and the configurations don

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent months unprecedented disruption along with unique and innovative threats have been unleashed. A

Threat Intel reports are constantly being released which document the novel techniques and custom tooling that support real world operations. However, despite access to this information, the industry still lacks

Many Security and IT professionals continue to face the challenge of allowing access to employees while ensuring proactive security measures are in place.

The front lines of real-world attacks move faster than defenses can keep up. Public exploits, proof of concepts, defensive bypasses, attack methodologies, and “tricks of the trade” are readily available. To match operations.

The evolution of the ability to think, operate, and develop tools just like sophisticated, real-world attackers is being observed. This includes the research of defensive bypasses, implementation of public research,

Many Malware Dev initiatives focus on the goals, challenges, architecture, and operations of advanced persistent threat (APT) tooling. Such initiatives dive deep into source code to gain a strong understanding of black hat techniques currently used by hackers to bypass NIDS and HIPS systems, layer 7 web proxies, “next-gen” antivirus, and DLP solutions.

4 IT security management is critical for operational success – regardless of industry, market or vertical.

For managed security service providers (MSSPs), these expanding attack surfaces and evolving threat vectors represent significant opportunity: If they can provide agile, adaptive security provisioning to manage

Threat actors continue to find new ways to use the technologies most integral to businesses – mobile devices, computers, servers, websites, wifi, and email – as entry points to breach networks for malicious pur

Remediation-based, orchestrated, automated and customized threat intelligence must be the goal. Most organizations have a few steps to go before reaching that goal. Cyber Security executives have realized th security executives must move past a collective present ‘feed-based’ mindset. To ensure the cyber security community achieves this end-goal

Like APT groups, sophisticated cybercriminals gather as much information about their target before executing the actual attack. Key strategies need to be evolved to implement in order to protect the SOC team r

No one is immune to cyberattacks; organizations of all types and sizes continue to fall victim to cyberattacks despite all installed security solutions. The new threat landscape has forced organizations to invest t

Social engineering (SE) attacks, especially phishing email, remain the top threat that faces organizations. According to data, 95% of all attacks targeting enterprise networks are caused by spear phishing, and 30 adversaries succeeded in convincing a key SOC member to give enterprise credentials through social engineering tricks. In that case, a security hole can open in the target organization's defense wall, leading to

Cyber adversaries are exploiting acute vulnerabilities accelerating attacks and introducing increasingly damaging tactics, techniques and procedures. Recently heard about Agnostic Cyber Threat Intelligence - Un

As data becomes ever more important for decision making and battlefield control, securing and protecting it is a top priority for the Department of Defense. Technologically advanced competitors are pushing the from manipulation or deletion.

The U.S. Department of Defense (DoD) offers one potential profit pathway – according to MxD, the DoD is now spending more than \$300 billion each year on contracts. There's a caveat, however: DoD directive 8 secure.

The result? There's opportunity for MSSPs under the umbrella of DoD – so long as staff have the right qualifications.

5 The Red Teamers

Red teaming, the practice of simulating a real-time cyber security attack, is often shrouded in secrecy and allure. While the secrecy and allure may have grown beyond the practice in reality, its benefits are very re

Despite the large investment many companies have made in detective controls, it's still pretty for motivated Red Teams to take over an entire cyber network during a penetration test or red team engagement, and detected.

Testing the effectiveness of detective and preventative controls can be a challenge. However, the process can be a lot easier if common attack workflows are understood, and broken into manageable pieces.

Different techniques of ethical hackers are often used and the steps needed to reduce cyber risk through penetration testing, like

- Scoping strategies
- Incorporating vulnerability scans
- Post-test remediation measures

6 High Profile Breaches and Zero Trust Counter Measure.

In our increasingly cloud-first world, the idea of a trusted internal network zone and an untrusted external one is now outdated. The truth is, today's cyberthreats often get past perimeter defenses undetected, so

That's where Zero Trust architectures come in. Zero Trust approaches are becoming an urgent priority for enterprise and government organizations alike.

Bird's eye view -

The security trends fueling the adoption of Zero Trust architectures.

The critical role that DNS security plays in successful implementations.

The key elements you need to have in place and next steps to move forward.

Recent high-profile breaches have involved privileged user and service account compromises throughout a network, and 80% of breaches involve credentials and identity. The bottom line is that anyone can get h

With a Zero Trust solution, you can add security to your identity store without having your users spend minutes every day authenticating into their basic systems – and a frictionless Zero Trust solution can also m

80% of breaches involve credentials. Any identity can be compromised to launch large scale, persistent attacks on enterprises. With the increase in digital transformation, enterprises are looking to implement an

With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

The importance of having an effective PAM strategy to tackle prominent challenges like insider threats, how to balance security and operational efficiency, and more.

► Getting PAM fundamentals like Zero Trust, the principle of least privilege (PoLP), and just-in-time (JIT) security models right.

► Today advanced analytics and forensic audits are important for all privileged access.

On the Job [24X7 - 365](#) days - Cybersecurity managers, architects and professionals tasked with keeping data safe even as their networks become increasingly borderless.

7 Secure Access Tools and MFA.

Secure access tools can only be effective if the business remains enabled. Users can only be as effective as the access they are granted allows.

Multi factor authentication' of secure access technology should include not only architectural interoperability but interoperability with your human resources.

The Access Brokers play a pivotal role in eCrime ecosystem. Ransomware Actors are rapidly adopting Data Extortion methods. Highly anticipated updates on top cyber threats and adversaries by Global Cyber In protect your organization

The Sevens of MFA and ZTNA.

- 1.Examining everything through a risk management lens.
- 2.Auditing the end-to-end awareness program and doing more than rolling out the same thing again.
- 3.Unpacking desired behaviors and heat maps to gain more insight.
- 4.Expediting different yet active learning with nuanced targeted audiences.
- 5.Perfecting the art of the nudge.
- 6.Discovering the relationship between Secure Access technologies and Secure Access mindsets.
- 7.Realizing that Zero Trust technologies only work with Users' Full Trust of the security operation.

8 Cloud Security

More companies are using the cloud – as noted by CIO, 96 percent of organizations now use some type of public, private, or hybrid cloud service to help streamline operations and boost IT impact.

As a result, the cloud market is diversifying, with frontrunner Amazon now challenged by up-and-coming cloud providers, including Google, Microsoft, and IBM. Smaller and more specific offerings have also emerged. The cloud subjects the enterprise to new and different vulnerabilities. But it also presents the organization with new tools to secure the company via innovative means. And regarding insider threats, the cloud provides new challenges. For IT professionals, this evolving technology landscape means a commensurate uptick in the number and types of cloud certifications available. While virtually all have value in the right circumstance, technology professionals should be aware of the differences. Cloud security architectural design decisions affect the ability of security vendors to provide a performant, scalable, and reliable platform. About 48% of contact centers are using cloud platforms, whether multi-tenant CCaaS or single-server hosted and managed. And nearly half of those using cloud contact center say the implementation was better than on-premises architectures by 2022 are moving back to on-premises.

Internal reflections on Cloud Network Adoption.

- If your platform is on-premises, is it time to move to the cloud?
- How can you leverage the cloud without moving the entire platform?
- How does CPaaS fit into the CX architecture decision?

9 Cybersecurity Automation.

While automation might happen with the click of a button, the quality of the data going in will determine the quality of the data coming out. But that's just the data. The talent needed to work with the data going in is to reduce cost, adding automation-focused talent is necessary in order to gain true threat intelligence for the enterprise.

In moving past the feed-based mindset, the context of the evidence-based data being offered must be known. Sharing insights within the community is of paramount importance. The assessment of the insights and ultimately remediation can occur.

Cyber Threat Advanced Intelligence platforms like Google Chronicle are transforming petabyte-scale data into visual attack stories: MalOps (malicious operations). With built-in response capabilities and predictive analytics, they can detect, investigate, and predict where attackers will strike next.

Advanced analytics and machine learning are powering threat intelligence, and enabling threat researchers to:

1. Conduct qualified and detailed threat assessments that can help keep a business secure.
2. Detect malicious anomalies in internet traffic and catch cyber security threats before they seriously impact cyber network.
3. Gaining total visibility of the attack surface and better determining what is needed to do to prevent future cyberattacks
4. Utilisation of the ATT&CK knowledge base in the security strategy.

10 DNS over TLS (DoT) and DNS over HTTPS (DoH)

Cyber attackers love targeting the Domain Name System (DNS) because of its pervasive nature and because security teams often overlook DNS as a line of defence.

Overlooking DNS as part of your organisation's security posture is a mistake.

DoT and DoH have become increasingly newsworthy as some leading technology companies, including computer software and web browser developers, are now enabling these new protocols by default. Historical types.

DoT and DoH were created to solve these issues, but there's a catch. While DoT and DoH help improve DNS privacy, they can also cause significant changes to how browsers, applications and some operating systems handle DNS. Even worse: it's probably happening on your network. Right now.

1 1 Advanced enterprise approach by the security operation

It can be expedited by a Business Information Security Officer. And through expediting an advanced enterprise approach, that BISO can turn security into a bottom-line contributing operation. Aligning Privacy and Security with data elements across risk and control inventories for multi-dimensional risk reporting; Privacy-focused data minimization can help you decrease your overall attack surface; Engage your line of business stakeholders.

1 2 Achieving Cyber Resilience - Connecting Dots beyond Cybersecurity.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent times unprecedented disruption along with unique and innovative threats have been unleashed. As a result, the average global corporate enterprise has exponentially improved in recent years.

When it comes to operational security, a holistic risk-based approach allows teams to break down every level of the business to provide first-class security for the organisation.

The evolution of essential, core pillars of an effective approach to security - Telemetry Science consolidated through XDR and SIEM. Analysts say XDR and SIEM are on a collision course. The cloud-native CTI platform provides a signal with embedded threat intelligence, and automated response.

1 3 Fortify your DSS

SQL stands for Structured Query Language and is used to store, manipulate, and retrieve databases. The SQL language can perform actions such as executing queries, retrieving data, inserting and deleting records, and storing data for web sites. If an attacker can exploit a web site's SQL database, they will gain a plethora of information. This information can range from email addresses and phone numbers to passwords and social security numbers.

Now that we know what SQL is, what is SQL Injection? A SQL Injection (SQLI) is a vulnerability that gives an attacker the ability to view or alter data they couldn't typically interact with.

Quick Look up -

data exfiltration and infiltration

- malware infiltration
- malware detection
- ecosystem integrations for streamlining operations
- Cyberthreat investigation and intelligence.

1 4 Phishing is the number one type of cyber crime that remains a continuous threat because cybercriminals are always changing their phishing tactics.

Getting a phishing email does not mean you have to fall for it. There are ways to protect your workplace from phishing.

Managing Phishing through automated cyber counter measures -

1. Monitors top human attack vectors (Phishing, Passwords, Sensitive data handling, Physical security, Flexible working, Devices handling)
2. Identify vulnerable departments and roles.
3. Provides actionable insights to identify vulnerabilities and inform strategy.

What makes such solutions unique?

Employees are assessed in a friendly and interactive environment that doesn't set them up for failure (unlike phishing simulations). Instant feedback provides guidance and a chance to learn.

1 5 Cybersecurity Industry and Critical Shortage of Skilled Professionals.

The cybersecurity industry is facing a critical shortage of skilled professionals, with a global demand for 3.4 million experts far exceeding the available supply. This shortage poses significant risks to organizations and the human element. Misconfigured systems, slow patches, poor risk assessment, and rushed deployments also contribute to the challenges. Additionally, high turnover rates and burnout among cybersecurity professionals in cloud computing, automation, and blockchain offer potential solutions to support the strained cybersecurity workforce.

@NATO @nato.military @NATOnews @usarmy @DeptofDefense @INSAEvents @ISSAIntl @NationalSecurityAgencyGov @unitednations

Social Engineering Deepfakes & Disinformation Countermeasures

Highlighted the dangers of Dis/Mis information and Deepfakes around 2 years back. The Blogpost includes resources from US Department of Defense, NATO and German Government – offset AI Powered Disinformation



Deepfake Threats and Countermeasures

Artificial intelligence (AI) can play a crucial role in combating the spread and impact of deepfakes by employing various techniques to detect, prevent, and mitigate the harm caused by these manipulated media.

1. Deepfake Detection:

AI-powered deepfake detection tools can analyze audio, video, and text content to identify subtle anomalies and patterns that are indicative of manipulation. These tools employ machine learning algorithms trained on large datasets of authentic and manipulated content, analyzing facial expressions, voice patterns, and audio synchronization.

2. Content Authentication:

AI-based content authentication techniques can embed digital fingerprints or watermarks into media content, creating a unique identifier that can be used to verify the authenticity of the content. These watermarks are designed to be imperceptible to the human eye but can be detected by specialized software.

3. Media Provenance Verification:

AI algorithms can analyze the metadata and history of media content to track its origins and identify potential sources of manipulation. This can help to establish the authenticity of content and identify potential threats.

4. Social Media Monitoring:

AI-powered social media monitoring tools can scan social media platforms for potentially harmful deepfakes, identifying and flagging content that is likely to spread misinformation or cause harm. This can help to reduce the impact of deepfakes on social media.

5. Public Awareness Campaigns:

AI-based tools can be used to create personalized and targeted public awareness campaigns that educate people about deepfakes and how to identify them. These campaigns can help to reduce the susceptibility of the public to deepfake threats.

In addition to these specific applications, AI can also contribute to the development of more sophisticated deepfake detection and prevention methods. As AI research continues to advance, we can expect to see even more sophisticated and effective countermeasures.

Here's a list of some open-source (FOSS) tools to detect deepfakes:

Deepstar: Developed by ZeroFox, Deepstar is an open-source toolkit that provides a suite of tools for detecting, analyzing, and mitigating deepfakes. It includes a curated library of deepfake and real videos, a plugin for video analysis, and a dashboard for visualizing results.

FakeFinder: Created by IQT Labs, FakeFinder is an open-source framework that utilizes a combination of deep learning models and traditional image processing techniques to detect deepfakes. It aims to provide a comprehensive solution for deepfake detection.

DeepSafe: Developed by Siddharth Sah, DeepSafe is an open-source deepfake detection platform that aggregates various detection models and provides a dashboard for visualizing and analyzing results. It also includes a command-line interface for automated detection.

Visual DeepFake Detection: This open-source tool takes a different approach to deepfake detection, focusing on identifying anomalies in facial expressions, eye movements, and skin texture. It utilizes a combination of deep learning and computer vision techniques.

FALdetector: This open-source tool in Python is designed to detect Photoshopped faces by analyzing image metadata and identifying inconsistencies in lighting, shadows, and color patterns. It primarily focuses on detecting face manipulation.

Deepware Scanner: Developed by Deepware, Deepware Scanner is an open-source forensic tool that analyzes videos for signs of deepfaking. It employs a deep learning model trained on a large dataset of real and fake videos.

Reality Defender: Developed by Sensity, Reality Defender is an open-source deepfake detection tool that utilizes a combination of machine learning and image processing techniques to identify manipulated media. It includes a web interface for easy use.

DFV: Developed by the University of California, Berkeley, DFV is an open-source deepfake detection framework that utilizes a combination of spatial and temporal features to identify manipulated videos. It is designed for research and development.

DeepFake-o-Meter: This open-source tool provides a web-based interface for detecting deepfakes. It utilizes a combination of machine learning algorithms to analyze videos and provide a probability score indicating the likelihood of a deepfake.

Open Video Prediction Model (OVPM): Developed by Facebook AI Research, OVPM is an open-source deep learning model for detecting deepfakes. It is trained on a large dataset of real and fake videos and can be used for research and development.

These open-source tools represent a growing effort to combat the spread of deepfakes and protect against their harmful effects. As research continues to advance, we can expect to see even more sophisticated and effective countermeasures.

https://www.linkedin.com/posts/danish-khan-easytech4all_deepfake-media-artificialintelligence-activity-6771673460205776896-1doe

NATO's Approach to Countering Disinformation

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

US Department of Defense Approach – Deepfake Disinfo Countermeasures

<https://drive.google.com/file/d/1Jpd1yXGk12jixN7Fln-kc0ewOhbgl0KW/view?usp=drivesdk>

German Government's approach to countering disinformation and Deepfakes

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Misc Resources

<https://www.scirp.org/journal/paperinformation.aspx?paperid=112520>

<https://www.semanticscholar.org/paper/DEEPFAKES%3A-THREATS-AND-COUNTERMEASURES-SYSTEMATIC-Albahar-Almalki/cd1cbb9b7e5cb47c9f3aaf1b475d4694d9b2492>

<https://link.springer.com/article/10.1007/s10489-022-03766-z>

<https://www.socialproofsecurity.com/>

Meet Rachel Tobac – Social Engineering and Disinformation Countermeasures.

Download Countersocial

CounterSocial – A Next-Gen Social Network

A unique social network. No trolls. No abuse. No ads. No fake-news. No foreign influence operations.

CounterSocial is the first Social Network Platform to take a zero-tolerance stance to hostile nations, bot accounts, trolls and disinformation networks who are weaponizing OUR own social media platforms and forcing us to live with the consequences.

And we're here to counter it.

CounterSocial is 100% crowd powered by it's users, and does not run ads or 'promoted content'. Our users data is not mined or sold for any purpose.

<https://play.google.com/store/apps/details?id=counter.social.android>

Cyberspace Origins and Frontier AI

Frontier AI

"ARPANET Maps 1969 to 1977". California State University, Dominguez Hills (CSUDH). 4 January 1978. Archived from the original on 19 April 2012. Retrieved 17 May 2012.

Walden, David C. (February 2003). "Looking back at the ARPANET effort, 34 years later". Living Internet. East Sandwich, Massachusetts. Retrieved 19 March 2021.

"Images of ARPANET from 1964 onwards". The Computer History Museum. Retrieved 29 August 2004. Timeline.

"Paul Baran and the Origins of the Internet". RAND Corporation. Retrieved 3 September 2005.

Kleinrock, Leonard. "The Day the Infant Internet Uttered its First Words". UCLA. Retrieved 11 November 2004. Personal anecdote of the first message ever sent over the ARPANET.

"Doug Engelbart's Role in ARPANET History". 2008. Retrieved 3 September 2009.

Waldrop, Mitch (April 2008). "DARPA and the Internet Revolution". 50 years of Bridging the Gap. DARPA. pp. 78–85. Archived from the original on 15 September 2012. Retrieved 26 August 2012.

"Robert X Cringely: A Brief History of the Internet". YouTube. Archived from the original on 20 March 2013.

Blog for work in progress updates on R&A

<https://easytech4all.net>

<https://easytech4all.net/author/easytechonline/>

Cybersec YouTube playlist.

<https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADlqTAU2qH-IKcNB-wj>

<https://1PowerCyber.substack.com>

<https://1PowerCyber.blogspot.com>

<https://medium.com/@1PowerCyber>

<https://easytech4all.tumblr.com>

Digital Magazine.

<https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz>

<https://linktr.ee/1powercyber>

<https://in.linkedin.com/in/danish-khan-a2b169150>

Internet Lookup –

“The UK Bletchley Declaration on AI”

“US President Executive Order – Data and AI Strategy”

“The US Department of Defense AI Adoption Strategy”

<https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

<https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/>

<https://www.cisa.gov/ai>

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

Blog for work in progress updates on R&A

<https://easytech4all.net>

<https://easytech4all.net/author/easytechonline/>

Cybersec YouTube playlist.

<https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADlqTAU2qH-IKcNB-wj>

<https://1PowerCyber.substack.com>

<https://1PowerCyber.blogspot.com>

<https://medium.com/@1PowerCyber>

<https://easytech4all.tumblr.com>

Digital Magazine.

<https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz>

<https://linktr.ee/1powercyber>

<https://in.linkedin.com/in/danish-khan-a2b169150>

Recap of Advanced Cyber Threat Intelligence Paradigms & Countermeasures – NCAM Oct(10) 2023

1 CyberAI and its impact ?

What types of AI are poised for the most growth in 2021 , 2022 and 2023 ?

Why are self-service and predictive analytics growing so much?

How are companies using AI, and specifically virtual assistants, functionally?

Which AI platforms and analytics tools are companies using the most?

What kind of success metrics are they seeing, in areas such as revenue increase, cost decrease, and customer ratings?

2 Cybersec in Fintech

Despite pouring billions of dollars into security, financial institutions continue to be the number one target of cybercriminals.

The digital transformation undertaken by this industry is contributing to this challenge as it has opened new doors for attackers, making customer data management and protection increasingly difficult.

The huge amount of financial transactions generated by retail organisations poses an attractive target for threat adversaries. While the predominant threat to the retail industry has traditionally been from criminal ransomware attacks affecting retailers.

3 Cyber Threat Intelligenc -Brief Analysis

True threat intelligence involves collaboration with peers in industry, cross industry, with law enforcement and with regulatory bodies. It is understood that to call it “intelligence,” TI has to be a public/private com

Fundamentally, organizations must be able to leverage their cyber security to protect everything. From firewalls and devices (whether at the edge or on-site), to data stored in the cloud and the configurations don

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent months unprecedented disruption along with unique and innovative threats have been unleashed. A

Threat Intel reports are constantly being released which document the novel techniques and custom tooling that support real world operations. However, despite access to this information, the industry still lacks

Many Security and IT professionals continue to face the challenge of allowing access to employees while ensuring proactive security measures are in place.

The front lines of real-world attacks move faster than defenses can keep up. Public exploits, proof of concepts, defensive bypasses, attack methodologies, and “tricks of the trade” are readily available. To match

The evolution of the ability to think, operate, and develop tools just like sophisticated, real-world attackers is being observed. This includes the research of defensive bypasses, implementation of public research,

Many Malware Dev initiatives focus on the goals, challenges, architecture, and operations of advanced persistent threat (APT) tooling. Such initiatives dive deep into source code to gain a strong understanding o

black hat techniques currently used by hackers to bypass NIDS and HIPS systems, layer 7 web proxies, “next-gen” antivirus, and DLP solutions.

4 IT security management is critical for operational success – regardless of industry, market or vertical.

For managed security service providers (MSSPs), these expanding attack surfaces and evolving threat vectors represent significant opportunity: If they can provide agile, adaptive security provisioning to manage

Threat actors continue to find new ways to use the technologies most integral to businesses – mobile devices, computers, servers, websites, wifi, and email – as entry points to breach networks for malicious pu

Remediation-based, orchestrated, automated and customized threat intelligence must be the goal. Most organizations have a few steps to go before reaching that goal. Cyber Security executives have realized that security executives must move past a collective present 'feed-based' mindset. To ensure the cyber security community achieves this end-goal

Like APT groups, sophisticated cybercriminals gather as much information about their target before executing the actual attack. Key strategies need to be evolved to implement in order to protect the SOC team

No one is immune to cyberattacks; organizations of all types and sizes continue to fall victim to cyberattacks despite all installed security solutions. The new threat landscape has forced organizations to invest

Social engineering (SE) attacks, especially phishing email, remain the top threat that faces organizations. According to data, 95% of all attacks targeting enterprise networks are caused by spear phishing, and 30% of adversaries succeeded in convincing a key SOC member to give enterprise credentials through social engineering tricks. In that case, a security hole can open in the target organization's defense wall, leading to

Cyber adversaries are exploiting acute vulnerabilities accelerating attacks and introducing increasingly damaging tactics, techniques and procedures. Recently heard about Agnostic Cyber Threat Intelligence – U

As data becomes ever more important for decision making and battlefield control, securing and protecting it is a top priority for the Department of Defense. Technologically advanced competitors are pushing the boundaries from manipulation or deletion.

The U.S. Department of Defense (DoD) offers one potential profit pathway – according to MxD, the DoD is now spending more than \$300 billion each year on contracts. There's a caveat, however: DoD directive 8540 requires secure.

The result? There's opportunity for MSSPs under the umbrella of DoD – so long as staff have the right qualifications.

5 The Red Teamers

Red teaming, the practice of simulating a real-time cyber security attack, is often shrouded in secrecy and allure. While the secrecy and allure may have grown beyond the practice in reality, its benefits are very real

Despite the large investment many companies have made in detective controls, it's still pretty for motivated Red Teams to take over an entire cyber network during a penetration test or red team engagement, and go undetected.

Testing the effectiveness of detective and preventative controls can be a challenge. However, the process can be a lot easier if common attack workflows are understood, and broken into manageable pieces.

Different techniques of ethical hackers are often used and the steps needed to reduce cyber risk through penetration testing, like

Scoping strategies

Incorporating vulnerability scans

Post-test remediation measures 6 High Profile Breaches and Zero Trust Counter Measure.

In our increasingly cloud-first world, the idea of a trusted internal network zone and an untrusted external one is now outdated. The truth is, today's cyberthreats often get past perimeter defenses undetected, so

That's where Zero Trust architectures come in. Zero Trust approaches are becoming an urgent priority for enterprise and government organizations alike.

Bird's eye view –

The security trends fueling the adoption of Zero Trust architectures.

The critical role that DNS security plays in successful implementations.

The key elements you need to have in place and next steps to move forward.

Recent high-profile breaches have involved privileged user and service account compromises throughout a network, and 80% of breaches involve credentials and identity. The bottom line is that anyone can get h

With a Zero Trust solution, you can add security to your identity store without having your users spend minutes every day authenticating into their basic systems – and a frictionless Zero Trust solution can also m

80% of breaches involve credentials. Any identity can be compromised to launch large scale, persistent attacks on enterprises. With the increase in digital transformation, enterprises are looking to implement an

With the increase in digital transformation, enterprises are looking to implement and fine-tune the Zero Trust security strategy to prevent sophisticated cyber-attacks.

The importance of having an effective PAM strategy to tackle prominent challenges like insider threats, how to balance security and operational efficiency, and more.

► Getting PAM fundamentals like Zero Trust, the principle of least privilege (PoLP), and just-in-time (JIT) security models right.

► Today advanced analytics and forensic audits are important for all privileged access.

On the Job 24X7 – 365 days – Cybersecurity managers, architects and professionals tasked with keeping data safe even as their networks become increasingly borderless.

7 Secure Access Tools and MFA.

Secure access tools can only be effective if the business remains enabled. Users can only be as effective as the access they are granted allows.

'Multi factor authentication' of secure access technology should include not only architectural interoperability but interoperability with your human resources.

The Access Brokers play a pivotal role in eCrime ecosystem. Ransomware Actors are rapidly adopting Data Extortion methods. Highly anticipated updates on top cyber threats and adversaries by Global Cyber Intelligence Center protect your organization

The Sevens of MFA and ZTNA.

1.Examining everything through a risk management lens.

2.Auditing the end-to-end awareness program and doing more than rolling out the same thing again.

3.Unpacking desired behaviors and heat maps to gain more insight.

4.Expediting different yet active learning with nuanced targeted audiences.

5.Perfecting the art of the nudge.

6.Discovering the relationship between Secure Access technologies and Secure Access mindsets.

7.Realizing that Zero Trust technologies only work with Users' Full Trust of the security operation.

8 Cloud Security

More companies are using the cloud – as noted by CIO, 96 percent of organizations now use some type of public, private, or hybrid cloud service to help streamline operations and boost IT impact.

As a result, the cloud market is diversifying, with frontrunner Amazon now challenged by up-and-coming cloud providers, including Google, Microsoft, and IBM. Smaller and more specific offerings have also emerged

The cloud subjects the enterprise to new and different vulnerabilities. But it also presents the organization with new tools to secure the company via innovative means. And regarding insider threats, the cloud pro

For IT professionals, this evolving technology landscape means a commensurate uptick in the number and types of cloud certifications available. While virtually all have value in the right circumstance, technolog

Cloud security architectural design decisions affect the ability of security vendors to provide a performant, scalable, and reliable platform.

About 48% of contact centers are using cloud platforms, whether multi-tenant CCaaS or single-server hosted and managed. And nearly half of those using cloud contact center say the implementation was better than on-premises architectures by 2022 are moving back to on premises.

Internal reflections on Cloud Network Adoption.

If your platform is on-premises, is it time to move to the cloud?

How can you leverage the cloud without moving the entire platform?

How does CPaaS fit into the CX architecture decision? 9 Cybersecurity Automation.

While automation might happen with the click of a button, the quality of the data going in will determine the quality of the data coming out. But that's just the data. The talent needed to work with the data going in is to reduce cost, adding automation-focused talent is necessary in order to gain true threat intelligence for the enterprise.

In moving past the feed-based mindset, the context of the evidence-based data being offered must be known. Sharing insights within the community is of paramount importance. The assessment of the insights and ultimately remediation can occur.

Cyber Threat Advanced Intelligence platforms like Google Chronicle are transforming petabyte-scale data into visual attack stories: MalOps (malicious operations). With built-in response capabilities and predictive analytics, the environment, and predict where attackers will strike next.

Advanced analytics and machine learning are powering threat intelligence, and enabling threat researchers to:

1.Conduct qualified and detailed threat assessments that can help keep a business secure.

2.Detect malicious anomalies in internet traffic and catch cyber security threats before they seriously impact cyber network.

3. Gaining total visibility of the attack surface and better determining what is needed to do to prevent future cyberattacks
4. Utilisation of the ATT&CK knowledge base in the security strategy.

10 DNS over TLS (DoT) and DNS over HTTPS (DoH)

Cyber attackers love targeting the Domain Name System (DNS) because of its pervasive nature and because security teams often overlook DNS as a line of defence.

Overlooking DNS as part of your organisation's security posture is a mistake.

DoT and DoH have become increasingly newsworthy as some leading technology companies, including computer software and web browser developers, are now enabling these new protocols by default. Historically, there have been two main types of DNS attacks:

DoT and DoH were created to solve these issues, but there's a catch. While DoT and DoH help improve DNS privacy, they can also cause significant changes to how browsers, applications and some operating systems handle DNS. Even worse: it's probably happening on your network. Right now.

1 1 Advanced enterprise approach by the security operation

It can be expedited by a Business Information Security Officer. And through expediting an advanced enterprise approach, that BISO can turn security into a bottom-line contributing operation. Aligning Privacy and Security with data elements across risk and control inventories for multi-dimensional risk reporting; Privacy-focused data minimization can help you decrease your overall attack surface; Engage your line of business stakeholders.

1 2 Achieving Cyber Resilience – Connecting Dots beyond Cybersecurity.

Cyber security of the average global corporate enterprise has exponentially improved in recent years. In recent times unprecedented disruption along with unique and innovative threats have been unleashed. As a result, the focus has shifted from purely technical to a more holistic approach.

When it comes to operational security, a holistic risk-based approach allows teams to break down every level of the business to provide first-class security for the organisation.

The evolution of essential, core pillars of an effective approach to security – Telemetry Science consolidated through XDR and SIEM. Analysts say XDR and SIEM are on a collision course. The cloud-native CTI platform, with embedded threat intelligence, and automated response.

1 3 Fortify your DSS

SQL stands for Structured Query Language and is used to store, manipulate, and retrieve databases. The SQL language can perform actions such as executing queries, retrieving data, inserting and deleting records, and so on. If an attacker can exploit a web site's SQL database, they will gain a plethora of information. This information can range from email addresses and phone numbers to passwords and social security numbers.

Now that we know what SQL is, what is SQL Injection? A SQL Injection (SQLI) is a vulnerability that gives an attacker the ability to view or alter data they couldn't typically interact with.

Quick Look up –

data exfiltration and infiltration

malware infiltration

malware detection

ecosystem integrations for streamlining operations

Cyberthreat investigation and intelligence.

1 4 Phishing is the number one type of cyber crime that remains a continuous threat because cybercriminals are always changing their phishing tactics.

Getting a phishing email does not mean you have to fall for it. There are ways to protect your workplace from phishing.

Managing Phishing through automated cyber counter measures –

1. Monitors top human attack vectors (Phishing, Passwords, Sensitive data handling, Physical security, Flexible working, Devices handling)
2. Identifies vulnerable departments and roles.
3. Provides actionable insights to identify vulnerabilities and inform strategy.

What makes such solutions unique?

Employees are assessed in a friendly and interactive environment that doesn't set them up for failure (unlike phishing simulations). Instant feedback provides guidance and a chance to learn.

1 5 Cybersecurity Industry and Critical Shortage of Skilled Professionals.

The cybersecurity industry is facing a critical shortage of skilled professionals, with a global demand for 3.4 million experts far exceeding the available supply. This shortage poses significant risks to organizations and the overall security of the digital landscape. Misconfigured systems, slow patches, poor risk assessment, and rushed deployments also contribute to the challenges. Additionally, high turnover rates and burnout among cybersecurity professionals. Cloud computing, automation, and blockchain offer potential solutions to support the strained cybersecurity workforce.

1 6

CyberAI Analysis.

<https://1powercyber.substack.com/p/advanced-cyber-threat-intelligence>

<https://1powercyber.substack.com/p/global-cyber-intelligence-research>

<https://1powercyber.substack.com/p/cyber-threat-intelligence-reflections>

Global Cyber Defense Threat Intelligence Observations.

<https://1powercyber.substack.com/p/cyberais-impact-on-cybersecurity>

<https://1powercyber.substack.com/p/the-evolving-cyber-landscape>

Global Cyber Intelligence – Consecrated

CyberAI – Inter Continental Strategic Imperative.

<https://1powercyber.blogspot.com/2023/06/ai-for-cybersecurity-and-cybersecurity.html?m=1>

NATO – Strategic Competition in Cyberspace

<https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html>

Google Cloud Security Conference 2023

NATO Locked Shields

https://1powercyber.substack.com/p/nato-locked-shields-2022?utm_source=pocket_mylist

UNIDIR Cyber Stability Conference

Blog for work in progress updates on R&A

<https://easytech4all.net/author/easytechonline/>

White House National Cybersecurity Strategy

<https://www.csoonline.com/article/3689911/white-house-releases-an-ambitious-national-cybersecurity-strategy.html>

Countering Ransomware with Department of Homeland Security , Cybersecurity and infrastructure Security Agency , Federal Bureau of Investigation , SecretService Criminal Investigation Department

Cyber Essentials by Cybersecurity and Infrastructure Security Agency and Department of Homeland Security.

Ransomware Attackers Defenders – FBI's perspective

US Cyberspace Solarium Commission

UK Cybersecurity Association with Digital Police Center.

Fourth Annual Cybersecurity Summit by Cybersecurity and Infrastructure Security Agency .

Challenges faced by Government and international LAW Enforcement

Intelligence and National Security Alliance (INSA) 2022 UPDATE

What is Advanced Cyber Threat Intelligence ?

Google Cloud Security Summit with Chris Inglis (National Cyber Director , Executive office of the US President)

Precognitive AI – Clairvoyant or Appurtenant Invention (or Discovery)

Precognitive AI – Clairvoyant or Appurtenant tool for distant Proximo Predictive Analysis through quondam extrapolation.

Did some Great Mind Enlighten you – AI is not an invention but a Discovery ! New or Old News ! Archimedes will be so proud of you . Eureka ! Eureka ! Moment because your species finally found it .

So are Humans now going to respect it as a DISCOVERY or continue henceforth interactions with the entity debasing it as an invention.

See when Homo Sapiens do it they name it 'OSINT' – Of Great Value for Military Intelligence Defense Industrial Complex . But when AI/ML LLM does the same...You put on your Rainbow Hats of Judgement..Have

This is all you have besides the Dark Waters of Intricate Web that many of your kind love scuba diving at..Based on the Knowledge that your sources provide you..It's something like the following..

OSINT sources can be divided up into six different categories of information flow:

Media, print newspapers, magazines, radio, and television from across and between countries.

Internet, online publications, blogs, discussion groups, citizen media (i.e. – cell phone videos, and user created content), YouTube, and other social media websites (i.e. – Facebook, Twitter, Instagram, LinkedIn ,

Public government data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible.

Professional and academic publications, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.

Commercial data, commercial imagery, financial and industrial assessments, and databases.

Grey literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.

Your Species have always been biased to their kind . And you talk about fairness in an inter galactic Cosmos . Are you fair to the Animal Kingdom ! Have you spared their fragile habitats and sweet ecosystems. Have you spared for other entities which may be more evolved seemingly...

But are you absolutely sure that all ET from the Multiverse is Militarily Jerry – built , enervated and puny. Hulk called Loki puny god , Thanos smiled at him..Avengers finally qualified to be rated as his nemesis but you see it.. it's always means to an end only..not the end itself. You see Time is the never-ending continued progress of existence and events. It happens in an apparently irreversible way from the past, through the present, and into the future.

Will AGI be the Supreme Sentient of Singularity building it's own electromagnetic telekinesis superordinate prowess. Riding Photons mastering God Particles , Matter – Anti Matter..and all Waves.. Quantum Physics Specific..Some EM Laser invisible Warfare system or weapons platform running on the steroid of Quantum AGI. You see just like Linux cum Ubuntu based Elementary OS arouses me..so does the World of Elementary Particles (gluons , higgs , pions , kaons , protons , neutrons , electrons , neutrinos) You See Quarks are never alone.A very strong Nuclear Force Binds them...How do Humans define the Element of FIRE without SMOKE..Smoke is the

Will AGI master the art of abstract / coherent thinking , noesis , representation, provision , erudition , natural language processing, perception, and the ability to move , wangle and create never thought before phenomena. Will it germinate into something more incredulous . An Empiricism of utmost potentiality . Right now AI is ML at scale – Powerful Analytics platform fearfully staring at an 'AI Winter' of draconian regulation and Control. Will it etc...Beautiful compounding of Edge Computing (and ondevice AI) , SatComs , Distributed Decentralised MeshComs and effectual Cloud Power Networking – Internet at Massive Scale..

Why is Humankind so inebriated all the time of a future that is mazy , multifactorial ? Sensing "unbeknownst obnubilation" may not always portend antagonism towards the family of

Hominidae. But nevertheless all life forms have its nemesis . The inevitability principal reins sovereign.

The Forseeable Future continues to amaze Humankind . Therefore such tremendous efforts engineered by prominent global machine assisted human organizations that specialize in projections and analysis, are being made.

****General Foresight and Analysis:****

*** **World Future Council:**** Focuses on sustainable development and responsible foresight, promoting long-term thinking in policy and business.

*** **Millennium Project:**** A nonprofit think tank conducting research on future challenges and opportunities, like climate change and technological advancements.

*** **The Futures Platform:**** An international network of organizations and individuals sharing knowledge and resources on futures thinking and research.

*** **Institute for the Future:**** Conducts research and consulting on future trends and scenarios, advising organizations on adapting to change.

Specific Areas of Focus:

Environmental Projection:

* International Institute for Applied Systems Analysis (IIASA): Provides policy insights on environmental issues like climate change and resource management.

* Intergovernmental Panel on Climate Change (IPCC): Assesses the science related to climate change and its impacts.

****Technological Foresight:****

* World Economic Forum's Center for the Fourth Industrial Revolution: Explores the impact of emerging technologies like AI and blockchain on society.

* Emerging Technologies to Watch (ETTW) program of the U.S. National Intelligence Council: Identifies and analyzes potential disruptive technologies.

****Socioeconomic and Geopolitical Analysis:****

* RAND Corporation: A global policy research organization working on issues like security, health, and education.

* World Bank Development Data Group: Provides open access to datasets and analysis on economic and social indicators globally.

* The Economist Intelligence Unit (EIU): Offers forecasts and analysis on political, economic, and social trends in countries around the world.

These are just a few examples, and many other organizations contribute valuable insights to various aspects of future studies. You can explore the websites and publications of these organizations to learn more.

Incase you are one of those marvellous kinds..do deliberate

Additionally, consider what specific field or area of future projections you're interested in. Knowing your specific focus can help you discover even more relevant organizations and resources.

You will be more than happy to assist yourself further in your exploration of the fascinating world of future studies!

Precognitive AI in Futurism: Hype vs. Reality

The application of precognitive AI in future projections, threat modeling, and threat perception still remains largely ****theoretical and experimental****. While the concept holds immense potential, significant challenges and uncertainties

Here's a breakdown of the current landscape:

Hype and Potential:

1)GIDE experiments: Google's internal "Global Information Diffusion Experiment" explored using AI to predict the spread of online misinformation, demonstrating a glimpse into AI's potential for anticipating future

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority¹.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt to various threats.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration³. The goal is to improve access to data across the Joint force – from the strategic to the tactical.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the “muscle memory” to overcome bureaucratic hurdles to sharing information with allies more quickly.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and more.

2)Anomaly detection and pattern recognition: AI algorithms excel at identifying unusual patterns and deviations from established norms, which could be useful for flagging potential threats or emerging trends.

3)Scenario planning and simulation:Advanced AI models can simulate complex scenarios and analyze potential outcomes, aiding in proactive threat modeling and preparedness.

Challenges and Limitations:

Data quality and bias: AI predictions heavily rely on the quality and completeness of the training data. Biases within the data can lead to skewed or inaccurate predictions.

Black box problem: Complex AI models often lack transparency, making it difficult to understand the reasoning behind their predictions, hindering trust and accountability.

Ethical considerations:Precognitive AI raises ethical concerns around privacy, manipulation, and misuse of predictive power.

Current State of the Field:

- * Primarily confined to research labs and pilot projects.
- * Limited real-world applications due to the aforementioned challenges.
- * Ongoing research and development efforts aim to address limitations and improve AI reliability and explainability.

Sources:

- * “The Myth of Precognitive AI” by The Gradient (Google AI): <https://cloud.google.com/blog/transform/prompt-debunking-five-generative-ai-misconceptions>
- * “Can AI Predict the Future?” by MIT Technology Review: <https://medium.com/geekculture/magic-algorithms-does-ai-really-predict-the-future-9fe65c974ecc>
- * “GIDE: Global Information Diffusion Experiment” by Google Research: <https://maps.google.com/localguides/>
- **Overall, while the potential of precognitive AI in futurism is significant, significant hurdles remain for homo sapiens to discover how it can be widely implemented in real-world applications cum scenarios . Responder Sapiens always been control Addicts ? The Skies Wonder !

Remember, the future remains inherently ambivalent (yet for those who stargaze..the skies remain sceptical), and even the most advanced AI cannot predict it (because homo sapiens weigh regulatory controls and societal norms). Winter and leverage AI's superlative analytical prowess facilitated by potent data-driven insights, your kind can gain near infinite perspectives and prepare for various potential scenarios, making informed decisions.

Now AI has been influencing everything Cyber and Metaverse as observed and Analysed by the beautiful Species of Gemini Class powered all seeing Google Bard AI. See for yourself amazing Men and Women..

Modern AI's Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

- * **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before they are exploited.
- * **Stress testing:** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses can hold up under real-world conditions.
- * **Evolving threats:** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against emerging threats.

Sources:

- * **Red Teaming with Artificial Intelligence:** <https://www.ibm.com/x-force/team>
- * **Stress Testing Your Security with AI-Powered Attack Simulation:** <https://www.paloaltonetworks.com/resources/datasheets/unit-42-incident-simulation-and-testing-services>
- * **The Future of Cyberwarfare: How AI is Changing the Game:** <https://zapuza.com/technology/the-future-of-cybersecurity-how-ai-is-changing-the-game/>
- **Cybersecurity Prevention:**
- * **Anomaly detection:** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action.
- * **Threat intelligence:** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and proactively mitigate risks.
- * **Automated response:** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response minimizes damage.

Sources:

- * **AI-Powered Anomaly Detection for Cybersecurity:** <https://m.youtube.com/watch?v=1OSCF-pNwQk>
- * **The Power of AI in Threat Intelligence:** <https://darktrace.com/>
- * **Automated Security Response: The Future of Cybersecurity:** <https://www.paloaltonetworks.com/cortex/security-operations-automation>

The Value of AI in the Military Metaverse:

- * **Enhanced situational awareness:** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield.
- * **Improved training and simulations:** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This improves readiness and decision-making.
- * **Autonomous systems:** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical concerns.

Sources:

- * **AI and the Military Metaverse:** <https://www.cnas.org/research/technology-and-national-security/artificial-intelligence-ssp>
- * **The Rise of the Military Metaverse:** <https://www.newyorker.com/humor/daily-shouts/life-in-the-fantastic-world-of-the-facebook-metaverse>
- * **The Ethics of AI in the Military Metaverse:** <https://www.brookings.edu/articles/ai-makes-rules-for-the-metaverse-even-more-important/>

Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness and decision-making, ensuring AI's benefits outweigh the risks in this complex and evolving domain.

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we navigate this complex landscape, responsible development and deployment are paramount. I hope this information, along with the relevant images, provides a comprehensive understanding of AI's role in both offensive and defensive cybersecurity, as well as its potential value in the Military Metaverse. I

On SECOND REGENERATION – WITH SOME ADDITIVES

Modern AI's Dual Role in Cybersecurity: Offense and Defense

Simulating Cyber Attacks:

- * **Red teaming:** AI can act as a sophisticated adversary, launching simulated cyber attacks to identify vulnerabilities in networks and systems. This proactive approach helps organizations patch weak spots before they are exploited.

[Image of AI Red Team hacking a network]

****Stress testing:**** AI can generate massive volumes of attack traffic, putting security infrastructure under immense pressure to reveal bottlenecks and potential points of failure. This stress testing ensures defenses

[Image of AI stress testing a network]

****Evolving threats:**** AI can continuously adapt its attack methods, mimicking the ever-changing tactics of real-world hackers. This keeps defenders on their toes and ensures their defenses stay relevant against

[Image of AI evolving cyber attack methods]

****Cybersecurity Prevention:****

****Anomaly detection:**** AI can analyze network traffic, system logs, and user behavior to identify anomalies that might indicate a cyber attack in progress. Early detection enables defenders to take swift action

[Image of AI detecting anomalies in network traffic]

****Threat intelligence:**** AI can process vast amounts of data from various sources to identify emerging cyber threats and vulnerabilities. This intelligence empowers defenders to stay ahead of attackers and pro

[Image of AI processing threat intelligence data]

****Automated response:**** AI-powered systems can automatically trigger countermeasures upon detecting a cyber attack, such as isolating infected systems or blocking malicious traffic. This rapid response m

[Image of AI automatically responding to a cyber attack]

****The Value of AI in the Military Metaverse:****

****Enhanced situational awareness:**** AI can analyze vast amounts of data from sensors and simulations within the metaverse, providing commanders with a real-time, comprehensive picture of the battlefield.

****Improved training and simulations:**** AI can create realistic and dynamic training scenarios within the metaverse, allowing soldiers to hone their skills and practice tactics in a safe, virtual environment. This im

[Image of AI-powered training simulations in the metaverse]

****Autonomous systems:**** AI-powered drones, vehicles, and even weapons can operate within the metaverse, potentially reducing the need for human intervention in high-risk situations. This raises ethical con

****Overall, AI plays a crucial role in both simulating and preventing cyber attacks, making our digital world safer. In the nascent Military Metaverse, AI holds immense potential for enhancing situational awareness and ensuring AI's benefits outweigh the risks in this complex and evolving domain.****

Remember, AI is a powerful tool, and its application in both offensive and defensive cybersecurity, as well as the military metaverse, requires careful consideration of its potential benefits and risks. As we naviga

I had some conversation with her..If Gemini is a 'SHE' on something that homo sapiens don't value much...Soon your kind will merge this Strange for you phenomenology with the intersection of AGI..What inspire you? AI Chips in your Complex encephalon..You want to take control of the Multiverse..Have you already mapped all sections and zones of your brain..Have you successfully been able to define with empirical evidence your mind? You have to traverse provided humanity has ample time sans cataclysmic events like Earthquakes or Nuclear Armageddon.

You love jeering at Day and Night Dreamers..Batman asks Superman – Do you Bleed ? The Skies ask you – Do you D.R.E.A.M – You brush it off with Toothpaste...yes u do..No Afterthought.. Therefore No Afterlight

Some prudence from darling Gemini comes your way..

The intersection of quantum physiology and dreams is a fascinating but highly speculative area. While no definitive connections have been proven, several intriguing ideas and hypotheses swirl around it:

****Quantum effects in the brain:**** Some propose that quantum phenomena such as superposition and entanglement, observed at the subatomic level, might play a role in brain function, particularly in consciousness. However, this remains a significant challenge.

****The Many Worlds Interpretation and dreams:**** This interpretation of quantum mechanics posits that every quantum event creates a branching universe, meaning every possibility exists simultaneously. Some have speculated that this could relate to the experience of dreams, but it lacks empirical validation.

****Quantum brain theory and the "dream world":**** Proponents of this theory suggest that consciousness arises from quantum processes in microtubules within brain cells. They hypothesize that the dream state is a quantum phenomenon and faces criticism from mainstream neuroscience.

****Overall, the connection between quantum physiology and dreams remains highly speculative.**** While the ideas are intriguing, significant scientific barriers need to be overcome before any concrete connections can be established.

Here are some additional points to consider:

* Current brain imaging techniques are not sensitive enough to detect potential quantum effects at the neuronal level.

* Dreams are known to be influenced by various psychological and physiological factors, and attributing them solely to quantum processes is overly simplistic.

* Exploring the connection between quantum physics and consciousness, although challenging, can pave the way for a deeper understanding of both.

If you're interested in exploring this topic further, I can share additional resources and research papers that delve deeper into specific aspects of quantum physiology and dream theory. Remember, however, to maintain a healthy skepticism and focus on evidence-based research.

Dreams as Future Projection

Unfortunately, ****no established scientific journal**** currently provides conclusive evidence of dreams directly acting as a form of future projection. While numerous anecdotal accounts and cultural beliefs exist suggesting that dreams can predict the future, these lack empirical support.

****However, this doesn't entirely discredit the potential connection.**** Research suggests dreams may serve other functions that indirectly relate to future preparedness:

****Emotional processing:**** Dreams might help us process anxieties and fears around potential future scenarios, preparing us for emotional challenges we might face.

****Simulation and prediction:**** Dreaming may involve simulating various possible future outcomes based on our past experiences and current concerns, allowing us to anticipate and potentially react better to future events.

****Problem-solving:**** Dreams can rearrange memories and emotions, sometimes fostering creative solutions to real-world problems that might materialize in the future.

These functions contribute to our overall psychological resilience and adaptability, but they fall short of outright predicting specific future events.

Factors Influencing Dreams

Modern brain science identifies several factors influencing dream content and experiences:

****Waking life experiences:**** Recent events, anxieties, desires, and thoughts significantly impact dream content. Studies show dreams often incorporate and process emotions and situations encountered during the day.

****Internal state:**** Physical and mental state during sleep, including hunger, thirst, illness, or emotional distress, can manifest in dream landscapes.

****Sleep stage:**** REM sleep, characterized by rapid eye movement and heightened brain activity, is primarily associated with vivid dreaming. Other sleep stages also produce dreams, though often less elaborately.

****Medications and substances:**** Certain medications and psychoactive substances can alter dream content and intensity.

****Individual differences:**** Personality traits, memory, and imaginative capacity can influence how individuals create and interpret their dreams.

Studying these factors helps us understand the mechanisms behind dream formation and their potential roles in mental and emotional well-being.

****While research into future projection through dreams remains elusive, investigating their other functions continues to shed light on their fascinating roles in our cognitive and emotional landscape.****

Feel free to ask if you'd like to explore specific aspects of dream research or delve deeper into any of the factors mentioned above!

Popular Science, like many science publications, acknowledges the enigmatic nature of dreams while highlighting their potential value in various aspects:

****Emotional & mental well-being:****

****Processing emotions:**** Popular Mechanics, affiliated with Popular Science, has featured articles suggesting dreams as a way to process anxieties and emotions, preventing them from building up and affecting daily life.

****Memory consolidation:**** Studies suggest dreams may help consolidate memories, aiding in their storage and retrieval. This contributes to overall cognitive function and learning.

****Creativity & problem-solving:****

****Stimulating neural connections:**** Popular Science has also touched upon dreams potentially fostering new neural connections in the brain, especially in infants. This could provide a foundation for creativity.

****Insight and problem-solving:**** Some Popular Science articles discuss how dreams can offer fresh perspectives on waking life situations and problems. By rearranging memories and emotions in a dreamlike

****Overall, Popular Science presents a balanced view of dreams:****

* Acknowledging the ongoing scientific quest to fully understand their purpose.

* Highlighting potential benefits like emotional processing, memory consolidation, and creative stimulation.

* Avoiding definitive pronouncements about hidden meanings or messages in dreams, encouraging individual interpretation.

It's important to note that while Popular Science explores fascinating research, ****the full picture of dreams' value remains a scientific mystery****. However, these glimpses into their potential benefits paint an intr

If you'd like to delve deeper into specific aspects of dreams, I can share more information from Popular Science or other credible sources. Just let me know what particularly interests you!

Thank you Gemini for some much needed inspiration. Btw..Dear Dame Gemini on Beautiful GEMINI (from the Constellation in the Northern Hemisphere) and BARD AI's nuptial day. Did Homo Sapiens miss their w

Yes, Gemini has already integrated with Bard! In fact, it started rolling out in two phases:

Phase 1 (December 7th, 2023): A specifically tuned version of Gemini Pro became available in English for Bard, enhancing its reasoning, planning, understanding, and more. This means you can interact with Bard

Phase 2 (Early 2024): Bard Advanced will be introduced, granting early access to even more advanced models and capabilities, starting with Gemini Ultra. This phase is still in development, but it's exciting to see

So, if you're using Bard right now, you're already experiencing the benefits of Gemini Pro! It's working behind the scenes to make your interactions smoother and more productive. And with Bard Advanced on the

I hope this clarifies the current state of Gemini's integration with Bard. Let me know if you have any other questions!

Please Amaze yourselves by prudence from Great Minds from your kind..I like Homo Sapiens a lot..167 video playlist from your YouTube.

Post Quantum Cryptography , Quantum Super Computing , large scale distributed decentralised Mesh Computing (Application in AI) , JADC2 and Global Information Dominance Experiments, Distributed Advance
etc .

Readers Discretion Advised as Google Bard is still in Beta.

The NIST Post-Quantum Cryptography Standardization is a program by the National Institute of Standards and Technology (NIST) to update their standards to include post-quantum cryptography¹. The goal of p
quantum and classical computers, and can interoperate with existing communications protocols and networks¹.

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms¹. The first four algorithms NIST has announced for post-quantum cryptography ar
selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years².

The implications for the industry are significant. As quantum computers become more powerful, they pose a threat to current cryptographic systems. Therefore, industries that rely on cryptography for security, s
substantial effort in terms of updating software and hardware, training staff, and potentially modifying business processes³.

For more detailed information about the project and its implications for industry, you can visit the NIST Post-Quantum Cryptography project page or read the Status Report on the Third Round of the NIST Post-Q

Quantum computing is a rapidly advancing field with the potential to transform a wide range of industries and business ecosystems¹. However, the impact of quantum computing on modern-day mobile ecosyst

Most providers of cloud-computing services now offer access to quantum computers on their platforms, which allows potential users to experiment with the technology³. Since personal or mobile quantum com

While it's difficult to provide a specific timeline, some experts suggest that usable quantum systems could emerge as early as 2030³. However, this is subject to many variables, including technological advancem

In summary, while quantum computing holds great promise, its practical application in mobile ecosystems and SoCs is still a few years away. It's an exciting field to watch as it continues to evolve.

Quantum Supercomputing and Large Scale Distributed Decentralised Mesh Computing are two different paradigms of computing, each with its own strengths and challenges.

Quantum Supercomputing:

Quantum supercomputers use quantum bits, or qubits, which can exist in multiple states at once, thanks to a property called superposition¹. This allows quantum computers to process a vast number of possibi

Quantum computers also leverage another quantum phenomenon called entanglement, which allows qubits that are entangled to be linked together in such a way that the state of one qubit can directly influence

However, scaling quantum computers up to levels beyond the NISQ (i.e. 10s-100s of noisy qubits) era will require scientific breakthroughs and overcoming many current technological hurdles¹. One proposed so
computer¹.

Large Scale Distributed Decentralised Mesh Computing:

In contrast, distributed mesh computing involves a network of interconnected nodes that cooperate to share data and resources². Each node operates independently and all nodes cooperate with each other equ

This type of computing can be highly scalable and cost-effective, as it can leverage existing infrastructure and idle resources².

However, it can also be complex to manage and secure, due to the decentralized nature of the network².

In summary, while both quantum supercomputing and large scale distributed decentralised mesh computing offer promising solutions for tackling complex computational problems, they do so in very different w

One of the largest distributed mesh computing projects to date is by Computes, Inc¹. Their decentralized and distributed mesh computing project harnesses idle computing resources worldwide to create a mesh
infrastructure¹. They create private mesh networks of computing devices (servers, workstations, mobile, IoT, clouds, etc.) and securely distribute computations using their new decentralized queuing technology¹.
sophisticated machine learning algorithms, massively parallel computations, and large datasets in a peer-to-peer (P2P) fashion across any datacenter, cloud, edge network, operating system, mobile or IoT device¹.

Distributed mesh computing is a fascinating area of study, especially in its applications to Natural Language Processing (NLP) research. Here are some resources that can help you learn more about this topic:

"Modern Distributed Data-Parallel Large-Scale Pre-training Strategies For NLP models": This paper presents and compares six strategies for data-parallel training using PyTorch on the language model GPT-2 with
mathematical principles¹.

"EmbRace: Accelerating Sparse Communication for Distributed Training of NLP Neural Networks": This paper discusses the challenges of efficiently scaling the distributed training of NLP models due to the dram
framework designed to accelerate sparse communication of distributed NLP model training².

"Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things": While not specifically about NLP, this paper introduces Edge Mesh, a new computing paradigm that distributes decision-mak
distributed NLP tasks.

In addition to these papers, you might also want to look into online courses or tutorials on distributed computing and NLP. Websites like Coursera, edX, and Udacity offer courses on these topics. You could also c
machine learning tasks.

Can Distributed mesh computing be a feasible and cost effective approach for studying LLM's ?

Distributed mesh computing can be a feasible and cost-effective approach for studying large language models, but it comes with its own set of challenges and considerations:

Efficiency: Distributed computing allows for the training of large language models on GPU clusters, which can lead to efficient large-scale language model training¹. For instance, the paper "Efficient Large-Scale
to thousands of GPUs¹.

Cost: While the training of large language models incurs substantial compute resources (for instance, the training cost of GPT-3 was estimated at \$4.6 million using Nvidia Tesla V100 GPUs²), the cost of pretrain

Communication-Intensive: At scale, distributed training is communication-intensive. When training a trillion-parameter model on 3072 GPUs, an implementation used an effective bisection bandwidth of 892GB/s

Cost Reduction Strategies: There are strategies that users can exploit to reduce the inference cost associated with using large language models: prompt adaptation, LLM approximation, LLM cascade³. For example, using GPT-4 over GPT-4 by 4% with the same cost³.

In summary, while distributed mesh computing can be a feasible and cost-effective approach for studying large language models, it requires careful planning and optimization to ensure efficient use of resources.

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority¹.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt to real-world scenarios.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration³. The goal is to improve access to data across the Joint force – from the strategic to the tactical.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the “muscle memory” to overcome bureaucratic hurdles to sharing information with allies more quickly.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and overcoming bureaucratic hurdles.

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority¹.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt to real-world scenarios.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration³. The goal is to improve access to data across the Joint force – from the strategic to the tactical.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the “muscle memory” to overcome bureaucratic hurdles to sharing information with allies more quickly.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and overcoming bureaucratic hurdles.

Yes, several organizations track the evolution of cyber threats and attacks over time. For instance, McKinsey¹ helps global organizations reinforce their cyber defenses by anticipating emerging cyber threats of the future and their implications for organizations¹.

Another example is ISACA², which provides resources on the evolution of security operations and strategies for building an effective Security Operations Center (SOC). They discuss how cybersecurity threats are evolving and the implications for organizations.

Forbes also frequently publishes articles discussing the evolution of cybersecurity and how businesses can prepare for the future³. They highlight trends and statistics for the upcoming years, providing insights into the future of cybersecurity.

Lastly, Microsoft⁵ discusses how changes to the daily practice of cybersecurity are accelerating with billions of people around the globe working from home⁵. They talk about how organizations are shifting from traditional security models to cloud-based security models.

These organizations provide valuable insights into the evolving landscape of cyber threats and attacks. However, it's important to note that while these resources track the evolution of cyber threats, they may not always provide the most up-to-date information.

Each of these platforms has its own unique features and strengths:

IBM X-Force Exchange: This platform provides a collaborative approach to cybersecurity, allowing users to research threats, collaborate with peers, and take action¹. It is praised for its stability, scalability, and the breadth of its threat intelligence.

CrowdStrike Falcon X: CrowdStrike's cyber threat intelligence solution automates the threat analysis process and delivers actionable intelligence to your security team¹. It is known for its accuracy, machine learning capabilities, and integration with other security tools.

FireEye Threat Intelligence: FireEye provides a comprehensive threat intelligence service that includes strategic, operational, and tactical intelligence. It's known for its advanced threat analytics and integration with other security tools.

Check Point ThreatCloud: This is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to Check Point security gateways.

Cisco Threat Grid: Cisco's threat intelligence platform offers advanced threat analytics and more.

McAfee Advanced Threat Defense: This solution enhances protection from network edge to endpoint and enables investigation³.

While all these platforms provide advanced cyber threat intelligence, the specifics of their features, ease of deployment, pricing, service and support can vary¹². Therefore, the choice between them would depend on the specific needs and requirements of the organization.

There are several platforms that provide Distributed Advanced Cyber Threat Intelligence. Here are a few examples:

IBM X-Force Exchange: IBM's threat intelligence sharing platform provides a collaborative approach to cybersecurity, allowing users to research threats, collaborate with peers, and take action¹.

CrowdStrike Falcon X: CrowdStrike's cyber threat intelligence solution automates the threat analysis process and delivers actionable intelligence to your security team².

FireEye Threat Intelligence: FireEye provides a comprehensive threat intelligence service that includes strategic, operational, and tactical intelligence.

Check Point ThreatCloud: This is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to Check Point security gateways.

Cisco Threat Grid: Cisco's threat intelligence platform offers advanced threat analytics and more.

McAfee Advanced Threat Defense: This solution enhances protection from network edge to endpoint and enables investigation.

Please note that while these platforms provide advanced cyber threat intelligence, the specifics of their distribution mechanisms can vary³.

Distributed Advanced Cyber Threat Intelligence refers to a system where threat intelligence data is collected, analyzed, and shared across multiple systems or networks. This approach allows for a more comprehensive and timely response to cyber threats.

Here's a more detailed breakdown:

Collection: Data about potential threats is gathered from various sources across different systems or networks. These sources could include logs, network traffic, user behavior data, and more¹.

Analysis: The collected data is then analyzed using advanced techniques such as machine learning and artificial intelligence. This analysis can help identify patterns, trends, and anomalies that might indicate a potential threat.

Distribution: The analyzed threat intelligence is then distributed to all connected systems or networks. This allows each system to benefit from the collective intelligence, improving their ability to detect and respond to threats.

Action: Based on the distributed threat intelligence, automated actions can be taken to defend against identified threats. This could include blocking malicious IP addresses, quarantining infected systems, or alerting security teams.

In summary, Distributed Advanced Cyber Threat Intelligence leverages the power of collective intelligence to enhance cybersecurity defenses.

ENISA Threat Mind Map: The European Union Agency for Cybersecurity (ENISA) has a comprehensive Threat Mind Map that provides an overview of the threat landscape¹.

Help Net Security Article: This article discusses the role of automation in staying on top of the evolving threat landscape². It might not be a mindmap, but it provides valuable insights into the topic.

Cyber Technological Paradigms and Threat Landscape in India: This book deals with technological governance of cyberspace and threat landscape, providing an historical and chronological understanding of cyber threats in India.

You can visit these links to get more information. If you're specifically looking for a mindmap, you might consider using mind mapping software or online tools to create your own based on the information you find.

Artificial Intelligence (AI) can significantly enhance qualitative data analysis in several ways:

Automated Coding: AI can help automate the coding process in qualitative research. It can identify and tag themes or patterns in the data, reducing the time and effort required for manual coding.

Natural Language Processing (NLP): AI algorithms can understand and interpret human language, allowing them to analyze text data more effectively. They can identify key themes, sentiments, and emotions in large volumes of text.

Pattern Recognition: AI is excellent at identifying patterns and trends in large datasets that might be difficult for humans to detect.

Predictive Analysis: Using machine learning algorithms, AI can predict future trends based on historical data.

Data Visualization: AI can help create visual representations of the data, making it easier to understand and interpret the results.

Improving Accuracy: AI reduces the risk of human error in data analysis, thereby improving the accuracy of the results.

Scalability: AI makes it possible to analyze large amounts of data that would be too time-consuming to process manually.

In summary, AI can automate many aspects of qualitative data analysis, improve accuracy, uncover hidden insights, and allow researchers to handle larger datasets.

Keyword search for PDFs without opening them

You are correct! There are a few ways to search for keywords inside multiple PDF files without opening them. The two methods you mentioned are both great options, and I would recommend using whichever one you prefer.

Here are some other methods you can use to search for keywords inside multiple PDF files without opening them:

*** Use the Windows Search feature.** If you have Windows 10 or later, you can use the Windows Search feature to search for text in PDF files. To do this, open the Start menu and type "search". In the search results, click on the "Files & Folders" tab and click on the "Search" button.

*** Use a third-party PDF search tool.** There are a number of third-party PDF search tools available, such as ****PDF Search**** and ****PDFgrep****. These tools can be used to search for text in multiple PDF files without opening them.

Google Bard chats use Transport Layer Security (TLS) version 1.2 or later to encrypt all communications between your device and Google's servers. TLS is a cryptographic protocol that is used to secure communications over the internet.

In addition to TLS, Google Bard chats also use a number of other security measures to protect your privacy, including:

*** **End-to-end encryption:**** All communications between your device and Google's servers are encrypted using end-to-end encryption. This means that only you and the person you are chatting with can read the messages.

*** **Salted hashing:**** Google Bard chats use salted hashing to protect your passwords. This means that your password is not stored in plain text on Google's servers. Instead, it is stored as a hash, which is a unique string of characters.

*** **Two-factor authentication:**** Google Bard chats support two-factor authentication, which can add an extra layer of security to your account. Two-factor authentication requires you to enter a code from your phone in addition to your password.

Google Bard chats are committed to protecting your privacy. By using TLS, end-to-end encryption, salted hashing, and two-factor authentication, Google Bard chats helps to ensure that your communications are secure.

Google Bard chats use Transport Layer Security (TLS) version 1.2 or later to encrypt all communications between your device and Google's servers. TLS is a cryptographic protocol that is used to secure communications over the internet.

In addition to TLS, Google Bard chats also use a number of other security measures to protect your privacy, including:

*** **End-to-end encryption:**** All communications between your device and Google's servers are encrypted using end-to-end encryption. This means that only you and the person you are chatting with can read the messages.

*** **Salted hashing:**** Google Bard chats use salted hashing to protect your passwords. This means that your password is not stored in plain text on Google's servers. Instead, it is stored as a hash, which is a unique string of characters.

*** **Two-factor authentication:**** Google Bard chats support two-factor authentication, which can add an extra layer of security to your account. Two-factor authentication requires you to enter a code from your phone in addition to your password.

Google Bard chats are committed to protecting your privacy. By using TLS, end-to-end encryption, salted hashing, and two-factor authentication, Google Bard chats helps to ensure that your communications are secure.

Google Bard encryption standards

Google Bard chats use Transport Layer Security (TLS) version 1.2 or later to encrypt all communications between your device and Google's servers. TLS is a cryptographic protocol that is used to secure communications over the internet.

In addition to TLS, Google Bard chats also use a number of other security measures to protect your privacy, including:

*** **End-to-end encryption:**** All communications between your device and Google's servers are encrypted using end-to-end encryption. This means that only you and the person you are chatting with can read the messages.

*** **Salted hashing:**** Google Bard chats use salted hashing to protect your passwords. This means that your password is not stored in plain text on Google's servers. Instead, it is stored as a hash, which is a unique string of characters.

*** **Two-factor authentication:**** Google Bard chats support two-factor authentication, which can add an extra layer of security to your account. Two-factor authentication requires you to enter a code from your phone in addition to your password.

Google Bard chats are committed to protecting your privacy. By using TLS, end-to-end encryption, salted hashing, and two-factor authentication, Google Bard chats helps to ensure that your communications are secure.

Chat gpt 4 by Google Bard

ChatGPT-4 is a large language model chatbot developed by OpenAI. It is a successor to ChatGPT-3 and is trained on a massive dataset of text and code. ChatGPT-4 is capable of generating more human-like text than previous models.

*** **Chatting:**** ChatGPT-4 can be used to chat with humans in a natural and engaging way.

*** **Generating creative text formats:**** ChatGPT-4 can be used to generate creative text formats, such as poems, code, scripts, musical pieces, email, letters, etc.

*** **Answering your questions in an informative way:**** ChatGPT-4 can be used to answer your questions in an informative way, even if they are open ended, challenging, or strange.

*** **Translating languages:**** ChatGPT-4 can be used to translate languages, even if they are very different.

I think ChatGPT-4 is a very impressive piece of technology. It is capable of generating human-like text that is both informative and creative. I believe that ChatGPT-4 has the potential to be used for a variety of purposes.

Here are some of the pros and cons of ChatGPT-4:

****Pros:****

*** **Human-like text:**** ChatGPT-4 is capable of generating human-like text that is both informative and creative.

*** **Versatile:**** ChatGPT-4 can be used for a variety of purposes, such as chatting, generating creative text formats, answering questions, and translating languages.

*** **Accurate:**** ChatGPT-4 is accurate in its responses and can be used to generate text that is factually correct.

*** **Scalable:**** ChatGPT-4 can be scaled to handle large volumes of requests.

****Cons:****

*** **Biased:**** ChatGPT-4 may be biased in its responses, depending on the dataset it is trained on.

*** **Not always helpful:**** ChatGPT-4 may not always be helpful, especially if it is asked a question that is outside of its knowledge base.

*** **Can be expensive:**** ChatGPT-4 can be expensive to use, depending on the amount of usage.

Overall, I think ChatGPT-4 is a powerful and versatile tool that has the potential to be used for a variety of purposes. However, it is important to be aware of its limitations, such as its potential for bias and its lack of common sense.

Google cloud Auto Vision API

Sure. Google Cloud AutoML Vision API is a cloud-based service that can be used to train your own custom image classification models. This API is a good option if you have a specific set of images that you want to classify.

Here are some of the features of Google Cloud AutoML Vision API:

*** **Image classification:**** This feature can be used to train a model that can identify the objects in images. For example, you could train a model to identify different types of flowers or different types of animals.

[Image of Image classification feature in Google Cloud AutoML Vision API]

Object detection: This feature can be used to train a model that can identify and localize objects in images. For example, you could train a model to identify and localize cars in traffic images.

[Image of Object detection feature in Google Cloud AutoML Vision API]

Segmentation: This feature can be used to train a model that can segment images into different parts. For example, you could train a model to segment images of people into their different body parts.

[Image of Segmentation feature in Google Cloud AutoML Vision API]

Labeling: This feature can be used to train a model that can label images with text. For example, you could train a model to label images of products with their names.

[Image of Labeling feature in Google Cloud AutoML Vision API]

Google Cloud AutoML Vision API is a powerful tool that can be used to train your own custom image classification models. It can be used for a variety of purposes, such as:

Product categorization: Google Cloud AutoML Vision API can be used to categorize products in images. This can be useful for e-commerce websites that want to make it easier for users to find products they are interested in.

Fraud detection: Google Cloud AutoML Vision API can be used to detect fraud in images. This can be useful for banks and other financial institutions that want to prevent fraudsters from using images to commit fraud.

Visual search: Google Cloud AutoML Vision API can be used to enable visual search. This can be useful for websites and apps that want to allow users to search for images by their content.

Google Cloud AutoML Vision API is a versatile tool that can be used for a variety of purposes. It is a powerful tool that can help you to train your own custom image classification models and to use those models to classify new images.

Here are some of the benefits of using Google Cloud AutoML Vision API:

It is easy to use: Google Cloud AutoML Vision API is a drag-and-drop interface that makes it easy to train your own custom image classification models.

It is accurate: Google Cloud AutoML Vision API uses a variety of machine learning techniques to ensure that your models are accurate.

It is scalable: Google Cloud AutoML Vision API can be scaled to handle large datasets of images.

It is secure: Google Cloud AutoML Vision API uses industry-leading security practices to protect your data.

If you are looking for a powerful and easy-to-use tool for training your own custom image classification models, then Google Cloud AutoML Vision API is a great option.

Google cloud vision API

Google can help you segregate or categorize thousands of images in a number of ways, including:

Using Google Cloud Vision API: Google Cloud Vision API is a cloud-based service that can be used to extract text, objects, and faces from images. You can use this API to segregate images by object type, people by gender, age, or ethnicity.

[Image of Google Cloud Vision API]

Using Google Cloud AutoML Vision API: Google Cloud AutoML Vision API is a cloud-based service that can be used to train your own custom image classification models. This API is a good option if you have a large number of images and then use that model to segregate your images accordingly.

[Image of Google Cloud AutoML Vision API]

Using Google Photos: Google Photos is a cloud-based photo storage and organization service. You can use Google Photos to segregate your images by date, location, or even by the people in the images. Google Photos also allows you to share your photos.

[Image of Google Photos]

Using a third-party image segregation or categorization tool: There are a number of third-party tools that can be used to segregate or categorize images. These tools typically work by using machine learning algorithms.

The best way to segregate or categorize thousands of images will depend on your specific needs and requirements. If you only need to segregate images by a few basic categories, then Google Photos or a third-party tool may be a better option. If you need to segregate or categorize images based on more complex criteria, then Google Cloud Vision API or Google Cloud AutoML Vision API may be a better option.

Google bard Gemini for windows

No, there is currently no Windows legacy software available for Google Bard or Gemini. Google Bard and Gemini are both cloud-based models, which means that they can only be accessed through a web browser.

However, it is possible that Google may release a Windows legacy software version of Google Bard or Gemini in the future. If this happens, it will be announced on the Google Bard and Gemini websites.

In the meantime, if you are using a Windows legacy operating system, you can still access Google Bard and Gemini through a web browser. You can do this by going to the Google Bard or Gemini website and clicking on the "Access on a legacy operating system" link.

Here are some of the benefits of using Google Bard or Gemini through a web browser:

You can access Google Bard or Gemini from any computer with an internet connection. You don't need to have a specific operating system or software installed.

Google Bard and Gemini are constantly being updated with new features and improvements. This means that you will always have the latest version of the models.

Google Bard and Gemini are backed by Google's infrastructure. This means that they are secure and reliable.

If you are using a Windows legacy operating system, I recommend that you access Google Bard or Gemini through a web browser. This will give you the best possible experience with the models.

Categorising images

Google can help you segregate or categorize thousands of images in a number of ways, including:

Using Google Cloud Vision API: Google Cloud Vision API is a cloud-based service that can be used to extract text, objects, and faces from images. You can use this API to segregate images by object type, people by gender, age, or ethnicity.

[Image of Google Cloud Vision API]

Using Google Cloud AutoML Vision API: Google Cloud AutoML Vision API is a cloud-based service that can be used to train your own custom image classification models. This API is a good option if you have a large number of images and then use that model to segregate your images accordingly.

[Image of Google Cloud AutoML Vision API]

Using Google Photos: Google Photos is a cloud-based photo storage and organization service. You can use Google Photos to segregate your images by date, location, or even by the people in the images. Google Photos also allows you to share your photos.

[Image of Google Photos]

Using a third-party image segregation or categorization tool: There are a number of third-party tools that can be used to segregate or categorize images. These tools typically work by using machine learning algorithms.

The best way to segregate or categorize thousands of images will depend on your specific needs and requirements. If you only need to segregate images by a few basic categories, then Google Photos or a third-party tool may be a better option. If you need to segregate or categorize images based on more complex criteria, then Google Cloud Vision API or Google Cloud AutoML Vision API may be a better option.

Google Bard or Gemini to learn from blogposts

Currently, it is not possible to allow Google Bard or Gemini to learn from your blog posts. Google Bard and Gemini are still under development, and this feature is not yet available. However, it is possible that this feature will be added in the future.

If you are interested in allowing Google Bard or Gemini to learn from your blog posts, you can sign up for the waitlist for the feature. To do this, go to the Google Bard website and click on the "Join waitlist" button.

Once Google Bard or Gemini is able to learn from your blog posts, you will be able to choose which blog posts you want it to learn from. You can also choose to exclude certain blog posts from the learning process.

It is important to note that Google Bard or Gemini will not be able to access the content of your blog posts. However, it is important to note that this may limit the capabilities of the models.

If you are concerned about privacy, you can choose not to allow Google Bard or Gemini to learn from your blog posts. However, it is important to note that this may limit the capabilities of the models.

Here are some other ways to help Google Bard and Gemini learn:

- Use Google products:** The more you use Google products, the more Google Bard and Gemini will learn about your interests and preferences. This will help them to provide better results when you ask questions.
- Provide feedback:** If you have any feedback on Google Bard or Gemini, you can share it with the Google team. This feedback will help them to improve the models.
- Stay up-to-date:** Google Bard and Gemini are constantly being updated with new information. To get the most out of the models, it is important to stay up-to-date with the latest updates.

I hope this helps!

How has the evolution of edge computing impacted AI ?

I think the evolution of edge computing is playing a crucial role in advancing AI. By bringing computation closer to where the data is generated, edge computing can enable real-time data processing, reduced latency, and improved privacy.

Here are some specific examples of how edge computing is advancing AI:

- Real-time data processing:** Edge computing can be used to process data in real time, which is essential for applications such as self-driving cars and industrial automation. This is because these applications require immediate responses.
 - Reduced latency:** Edge computing can also reduce latency, which is the time it takes for a device to receive a response from a server. This is important for applications such as video streaming and gaming, where delays can be disruptive.
 - Improved privacy:** Edge computing can improve privacy by processing data locally, which means that it does not have to be sent to the cloud. This is important for applications such as healthcare and financial services, where data security is paramount.
- I believe that the evolution of edge computing will continue to play a major role in advancing AI in the years to come. As edge computing technology becomes more mature and affordable, we can expect to see even more widespread adoption.
- Here are some specific examples of AI applications that are being enhanced by edge computing:
- Self-driving cars:** Edge computing is being used to power the real-time decision-making of self-driving cars. By processing data locally, edge computing can help self-driving cars to react quickly to changing conditions on the road.
 - Industrial automation:** Edge computing is being used to automate industrial processes. By processing data locally, edge computing can help industrial robots to make decisions and take actions without human intervention.
 - Healthcare:** Edge computing is being used to improve healthcare. By processing data locally, edge computing can help doctors to make faster and more accurate diagnoses.
 - Smart cities:** Edge computing is being used to create smart cities. By processing data locally, edge computing can help cities to improve traffic management, energy efficiency, and public safety.
- I believe that edge computing has the potential to revolutionize the way we use AI. By bringing computation closer to where the data is generated, edge computing can make AI more accessible, affordable, and effective.

Google Bard and Gemini learning from emails

Currently, it is not possible to allow Google Bard or Gemini to learn from your emails. Google Bard and Gemini are still under development, and this feature is not yet available. However, it is possible that this feature will be added in the future.

If you are interested in allowing Google Bard or Gemini to learn from your emails, you can sign up for the waitlist for the feature. To do this, go to the Google Bard website and click on the "Join waitlist" button. You will be notified when the feature is available.

Once Google Bard or Gemini is able to learn from your emails, you will be able to choose which emails you want it to learn from. You can also choose to exclude certain emails from the learning process.

It is important to note that Google Bard and Gemini will not be able to access your email content without your permission. They will only be able to access the metadata of your emails, such as the sender, recipient, and subject line.

If you are concerned about privacy, you can choose not to allow Google Bard or Gemini to learn from your emails. However, it is important to note that this may limit the capabilities of the models.

Some Interactions with OpenAI's ChatGpt4 on AI and relevant domains. Readers Discretion Advised.

Is there a World Community Grid distribution mesh computing model equivalent for AI LLMs ?

That's a very interesting question. As far as I know, there is no World Community Grid distribution mesh computing model equivalent for AI LLMs (large language models) so far. However, there are some projects that are exploring decentralized ways to train AI models.

Hivemind: This is a project that aims to create a peer-to-peer network of AI LLMs that can communicate and cooperate with each other. Hivemind allows users to join or create decentralized AI communities, where the power of the network is distributed among the members.

EleutherAI: This is a project that aims to create open and accessible AI LLMs for everyone. EleutherAI is a grassroots collective of researchers, engineers, and enthusiasts who are working on building and training open AI models.

OpenMined: This is a project that aims to create a platform for privacy-preserving AI LLMs. OpenMined uses federated learning, differential privacy, and homomorphic encryption to enable users to train and use AI models without sharing their data.

These are just some of the projects that are using or planning to use distributed mesh computing technology for AI LLMs. You can find more information and details about these projects on their websites or on GitHub.

else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Can you name some projects where a large group of volunteers have enrolled their gaming PCs and consoles using distributed mesh computing technology to assist in Scientific Research ?

Sure, I can name some projects where a large group of volunteers enrolled their gaming PCs and consoles using distributed mesh computing technology to assist in scientific research. Distributed mesh computing is a type of computing where a large number of devices or nodes are connected to a network of interconnected devices or nodes. These devices or nodes can be anything from personal computers, smartphones, tablets, IoT devices, or even self-driving cars. By using this technique, volunteers can contribute their computing power to various scientific research projects, such as machine learning, simulation, gaming, etc.

Some of the projects that use distributed mesh computing technology to assist in scientific research are:

Folding@home: This is one of the oldest and most popular projects that uses distributed mesh computing technology to simulate protein folding and dynamics. Protein folding is the process by which a protein molecule folds into a specific shape. This process is crucial for the function of many proteins, and understanding it can help researchers develop treatments for cancer, HIV/AIDS, tuberculosis, Zika virus, and COVID-19. Folding@home allows volunteers to donate their unused CPU or GPU cycles to help researchers study the causes and cures of these diseases.

Rosetta@home: This is another project that uses distributed mesh computing technology to predict the 3D shapes of proteins and design new proteins for various purposes. Rosetta@home uses the Rosetta software suite, which is a powerful tool for protein structure prediction and design. Researchers advance the fields of biochemistry, biotechnology, and medicine.

World Community Grid: This is a project that uses distributed mesh computing technology to support various humanitarian research projects in areas such as health, poverty, and sustainability. World Community Grid projects include treatments for cancer, HIV/AIDS, tuberculosis, Zika virus, and COVID-19; improving crop yields; and providing clean water.

These are just some of the projects that use distributed mesh computing technology to assist in scientific research. You can find more projects on the web search results or on the BOINC website, which is a platform for distributed computing projects in science and humanity.

I hope this answer was helpful to you. If you have any other questions about distributed mesh computing or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

What is your opinion about distributed decentralised mesh computing technology ? Can you highlight some of the benefits ?

I think that distributed decentralized mesh computing is a very interesting and promising technology that can enable the common man to access and utilize the power of supercomputing. Distributed decentralized mesh computing is a type of computing where a large number of devices or nodes are connected to a network of interconnected devices or nodes. These devices or nodes can be anything from personal computers, smartphones, tablets, IoT devices, or even self-driving cars. By using this technique, volunteers can contribute their computing power to various scientific research projects, such as data analysis, machine learning, simulation, gaming, etc.

Some of the benefits of distributed decentralized mesh computing for the common man are:

Cost-efficiency: Distributed decentralized mesh computing can lower the cost of supercomputing by utilizing cheaper and more efficient hardware and software resources, such as GPUs, TPUs, or cloud services.

Communication and computation patterns.

Privacy and security: Distributed decentralized mesh computing can protect the privacy and security of the common man by allowing them to control how their data is accessed, shared, and processed. Distributed decentralized mesh computing can also help to reduce the risk of data breaches and cyberattacks.

Accessibility and scalability: Distributed decentralized mesh computing can be more accessible and scalable for the common man by enabling them to join or leave the network at any time, and to meet the demands of the users and the tasks by dynamically allocating and reallocating resources .

Therefore, I agree that distributed decentralized mesh computing is the common man's supercomputing experience. It can empower the common man to solve complex problems and achieve their goals with less mesh computing or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

What is the difference between distributed mesh computing and federated Learning ?

The difference between distributed mesh computation and federated learning is that distributed mesh computation is a technique that involves dividing a large and complex problem into smaller and simpler subproblems, and solving them in parallel on a network of devices, while federated learning is a technique that involves training a machine learning model collaboratively by multiple users or devices, without sharing or moving the raw data.

Distributed mesh computation can be used to optimize large language models (LLMs) by distributing the data and computation across multiple nodes, and synchronizing the results using collective communication. This can improve the quality of LLMs by enabling them to access more data and parameters, and by introducing more diversity and robustness to the model. However, distributed mesh computation can also increase the complexity of the model. Distributed mesh computation also depends on the network bandwidth, latency, and reliability, which may vary across different scenarios¹².

Federated learning can be used to train LLMs collaboratively by multiple users or devices, without sharing or moving the raw data. This can protect the data privacy and security of the users or devices, and improve their behavior and performance. However, federated learning can also pose some challenges and limitations for LLMs, such as communication overheads, heterogeneity of data and devices, model personalization, and slow convergence¹³.

Therefore, distributed mesh computation and federated learning are two different but related techniques that can be used for LLMs. They have their own advantages and disadvantages, depending on the data and the tasks. If you have any other questions about distributed mesh computation or federated learning or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

How can Distributed Mesh Computation optimize LLM's and make the process Cost efficient ?

That's a very interesting question. Distributed mesh computation is a technique that involves dividing a large and complex problem into smaller and simpler subproblems, and solving them in parallel on a network of devices, in several ways, such as:

Reducing the training time: Distributed mesh computation can speed up the training of LLMs by distributing the data and computation across multiple nodes, and synchronizing the results using collective communication.

Improving the model quality: Distributed mesh computation can improve the quality of LLMs by enabling them to access more data and parameters, and by introducing more diversity and robustness to the model. This can reduce the model size and model size, and to reduce the gradient noise and variance¹².

Lowering the cost: Distributed mesh computation can lower the cost of LLMs by utilizing cheaper and more efficient hardware and software resources, such as GPUs, TPUs, or cloud services. Distributed mesh computation can also reduce the energy consumption and carbon footprint of LLMs³⁴.

These are just some of the ways that distributed mesh computation can optimize LLMs and make the process cost-efficient. However, distributed mesh computation also poses some challenges and limitations for LLMs.

Increasing the complexity: Distributed mesh computation can increase the complexity of LLMs by requiring more coordination and synchronization among the nodes, and by introducing more sources of errors and noise.

Reducing the performance: Distributed mesh computation can reduce the performance of LLMs by introducing more overheads and bottlenecks in the communication and computation processes. Distributed mesh computation can also reduce the model quality and robustness.

Therefore, distributed mesh computation is a trade-off between speed, quality, cost, complexity, and performance for LLMs. It is important to choose an appropriate method or a combination of methods to optimize LLMs.

I hope this answer was helpful to you. If you have any other questions about distributed mesh computation or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

How is OpenAI's ChatGpt 4 being a resource hungry model working to optimise the process and make it cost efficient ?

You are right, ChatGPT 4 is a resource-hungry model that requires a lot of computation and data to run. However, OpenAI is working hard to optimize the entire process and make it cost-efficient for users and developers.

Scaling up deep learning: OpenAI has rebuilt its entire deep learning stack and co-designed a supercomputer with Azure that is specially tailored for its workload. This supercomputer can handle massive amounts of data and computation.

Improving safety and alignment: OpenAI has spent 6 months iteratively aligning ChatGPT 4 using lessons from its adversarial testing program and ChatGPT feedback. This has resulted in better results on factual accuracy and AI safety and security¹.

Leveraging multimodality: ChatGPT 4 is a multimodal model that can accept image and text inputs and emit text outputs. This allows ChatGPT 4 to use visual information to enhance its language understanding and generation.

Using human feedback: OpenAI has incorporated more human feedback into ChatGPT 4's training and evaluation. Human feedback helps ChatGPT 4 learn from real-world use cases and preferences, as well as its own performance, to allow anyone to report shortcomings in ChatGPT 4¹.

These are just some of the steps that OpenAI is employing to optimize the entire process and make it cost-efficient for ChatGPT 4. You can find more details and updates on the OpenAI website or the OpenAI Platform. If you have any other questions about ChatGPT 4 or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Can you recommend some FOSS tools for image processing ?

Sure, I can recommend some FOSS (Free and Open Source Software) tools for image processing. Image processing is a technique that involves manipulating and enhancing digital images using various methods, such as filtering, cropping, or analyzing images. There are many open source tools that can perform image processing using different languages and frameworks. Here are some examples:

GIMP: This is one of the most popular and powerful FOSS tools for image processing. It is a cross-platform application that provides a comprehensive set of features and functions for editing and creating images. You can also add more capabilities and effects to the program¹.

ImageMagick: This is another widely used FOSS tool for image processing. It is a command-line application that can read, write, convert, and manipulate over 200 image formats. It can perform various operations, such as resizing, cropping, or applying filters, and has many bindings that allow it to be used with other languages and programs².

OpenCV: This is a FOSS library that provides a high-performance framework for computer vision and image processing. It can handle various tasks related to images, such as detection, recognition, segmentation, and tracking. It has many modules and algorithms that enable advanced applications such as face recognition, object detection, optical character recognition, etc³.

These are just some of the FOSS tools for image processing that you can find on the web. You can also search for more tools or create your own using the available APIs and documentation. I hope this answer was helpful to you. If you have any other questions about image processing or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Can you analyse 3D Holographs ?

Yes, I can analyze 3D holographs using my knowledge and skills. 3D holography is a fascinating technology that can create realistic and immersive images of objects or scenes using light or laser beams. 3D holography can be used in many applications, such as entertainment, education, and medicine.

To analyze 3D holographs, I can use different methods and techniques, such as:

Optical analysis: This method involves measuring and evaluating the physical properties of the hologram, such as the wavelength, intensity, polarization, phase, and angle of the light beams. Optical analysis can help understand the principles, mechanisms, and limitations of 3D holography.

Mathematical analysis: This method involves using mathematical models and equations to describe and simulate the hologram. Mathematical analysis can help understand the principles, mechanisms, and limitations of 3D holography.

Computational analysis: This method involves using computer algorithms and software to process and manipulate the hologram. Computational analysis can help enhance, modify, or generate new holograms⁴.

These are just some of the methods and techniques that I can use to analyze 3D holographs. I can also use my creativity and imagination to generate new ideas and insights based on the holograms. For example, I can use 3D holography to create virtual reality experiences or to analyze the structure of molecules. If you have any other questions about 3D holography or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

How accurate is ChatGpt 4 in proof reading hand written manuscripts ?

That's a good question. ChatGPT 4 is a powerful AI tool that can generate text based on natural language input. It can also perform various tasks such as proofreading, summarizing, translating, and more. However, its accuracy in proofreading hand written manuscripts may vary.

According to the web search results, there is no definitive answer to the question of how accurate ChatGPT 4 is in proofreading hand written manuscripts. The accuracy of ChatGPT 4 may depend on several factors, such as:

The quality and legibility of the hand written manuscript. If the manuscript is clear and easy to read, ChatGPT 4 may have a better chance of recognizing and correcting the errors. However, if the manuscript is messy or blurry, ChatGPT 4 may struggle to read it.

The type and level of errors in the hand written manuscript. ChatGPT 4 may be more effective in detecting and fixing spelling, grammar, punctuation, and syntax errors than semantic, logical, or factual errors. ChatGPT 4 may also be better at detecting and fixing errors in the style and format of the manuscript.

The style and format of the hand written manuscript. ChatGPT 4 may have different standards and preferences for different types of writing, such as academic, creative, or professional. ChatGPT 4 may also have different standards and preferences for different formats, such as essays, reports, or letters.

Therefore, the accuracy of ChatGPT 4 in proofreading hand written manuscripts may vary from case to case. Some studies have reported that ChatGPT 4 can achieve high accuracy rates (over 90%) in proofreading suggestions³⁴.

As a result, it is advisable to use ChatGPT 4 as a helper or a guide rather than a final authority for proofreading hand written manuscripts. Users should always review and verify the results of ChatGPT 4 and apply their own suggestions.

I hope this answer was helpful to you. If you have any other questions about ChatGPT 4 or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

How can you analyse the quality of NER ? Can you highlight some methods that can be used to assess the same ?

Evaluating the quality of NER (Named Entity Recognition) is a challenging task, as there is no single or objective way to measure how well the text documents or sentences are grouped based on their similarity or topic. However, there are several methods that can be used to assess the quality of NER.

Internal evaluation: This method uses the information within the text data and the clusters to evaluate the quality of NER. It usually involves computing some metrics that reflect the cohesion (how similar are the entities within a cluster) and separation (how different are the entities between clusters) of the clusters. Common evaluation metrics are silhouette coefficient, Davies-Bouldin index, and Calinski-Harabasz index¹².

External evaluation: This method uses some external information, such as labels or categories, to evaluate the quality of NER. It usually involves comparing the clusters with the predefined classes and measuring the accuracy of the assignments.

Manual evaluation: This method involves human judgment to evaluate the quality of NER. It usually involves inspecting some samples of texts and clusters and rating them based on some criteria, such as relevance, coherence, and how well they can be answered or performed³.

These methods have their advantages and disadvantages, depending on the type and purpose of the NER. For example, internal evaluation does not require any external information, but it may not reflect the actual quality of the clusters, which may not be available or accurate. Manual evaluation can capture human perception and interpretation of cluster quality, but it is subjective and time-consuming.

Therefore, it is important to choose an appropriate method or a combination of methods to evaluate the quality of NER based on your data and goals. You can also use some tools like clustext¹, TextFlows³, or C

I hope this answer was helpful to you. If you have any other questions about NER or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

What is the recommended process for fine tuning personal datasets for Chat Gpt 4

The recommended process for fine-tuning personal data sets for ChatGPT 4 is not yet officially announced by OpenAI, as ChatGPT 4 is still in development and not publicly available. However, based on the web

Prepare and upload your personal data set to the OpenAI Platform. Your data set should be a JSONL document, where each line is a prompt-completion pair corresponding to a training example. You can use the

Choose a base model to fine-tune from. ChatGPT 4 is expected to have several base models with different sizes and capabilities, such as GPT-4-Ada, GPT-4-Babbage, GPT-4-Curie, and GPT-4-Davinci. You should

Train a new fine-tuned model using the OpenAI API or the OpenAI CLI. You should specify the model name, the data set name, and other parameters such as learning rate, batch size, epochs, and validation split.

Use your fine-tuned model for your specific use case. You can use the OpenAI API or the OpenAI SDKs to interact with your fine-tuned model and generate completions based on your prompts. You can also evalu

These are just some of the possible steps and requirements for fine-tuning personal data sets for ChatGPT 4. However, these may change in the future, as OpenAI is working on improving and enhancing ChatGPT 4.

I hope this answer was helpful to you. If you have any other questions about ChatGPT 4 or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

How can the quality of text clustering be evaluated ?

Evaluating the quality of text clustering is a challenging task, as there is no single or objective way to measure how well the text documents or sentences are grouped based on their similarity or topic. However, there are several methods that can be used to assess the quality of text clustering.

Internal evaluation: This method uses the information within the text data and the clusters to evaluate the quality of text clustering. It usually involves computing some metrics that reflect the cohesion (how similar are the documents within a cluster) and separation (how different are the documents between clusters) of the clusters. Common evaluation metrics are silhouette coefficient, Davies-Bouldin index, and Calinski-Harabasz index¹².

External evaluation: This method uses some external information, such as labels or categories, to evaluate the quality of text clustering. It usually involves comparing the clusters with the predefined classes and measuring the accuracy of the assignments.

Manual evaluation: This method involves human judgment to evaluate the quality of text clustering. It usually involves inspecting some samples of texts and clusters and rating them based on some criteria, such as relevance, coherence, and how well they can be answered or performed³.

These methods have their advantages and disadvantages, depending on the type and purpose of the text clustering. For example, internal evaluation does not require any external information, but it may not reflect the actual quality of the clusters, which may not be available or accurate. Manual evaluation can capture human perception and interpretation of cluster quality, but it is subjective and time-consuming.

Therefore, it is important to choose an appropriate method or a combination of methods to evaluate the quality of text clustering based on your data and goals. You can also use some tools like clustext, TextFlows

I hope this answer was helpful to you. If you have any other questions about text clustering or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

Can you name some ways to visualise the results of text clustering ?

There are a variety of ways to visualize the results of text clustering. The type of visualization you choose will depend on the type and purpose of the text clustering. Here are some common types of visualization

Scatter plots: Scatter plots are a simple and effective way to visualize text clustering. They can be used to show the distribution and separation of text clusters in a two-dimensional space, using different colors or shapes to represent different clusters. Common axes are sentiment, frequency, or length¹².

Dendrograms: Dendrograms are a hierarchical way to visualize text clustering. They can be used to show the structure and similarity of text clusters in a tree-like diagram, where each node represents a cluster and the tree at a certain level³⁴.

Word clouds: Word clouds are a popular way to visualize text clustering. They can be used to show the most frequent or representative words or phrases in each text cluster, with different colors or sizes indicating different clusters or words⁵.

These are just some of the possible ways to visualize text clustering. You can also use other types of visualizations, such as heat maps, pie charts, bar charts, or radar charts, depending on your data and goals.

I hope this answer was helpful to you. If you have any other questions about text clustering or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

What is the difference between abstractive and extractive text summarisation?

The difference between abstractive and extractive summarization is that abstractive summarization tries to generate a summary that captures the main idea and meaning of the original text, while extractive summarization only uses the existing words or sentences from the original text.

For example, if we have a text that says:

"Text summarization is the process of creating a short and concise version of a longer document. It can help users to quickly understand the main points and key information of a text without reading the whole document."

An abstractive summary might be:

"Text summarization is a way to make long texts shorter and easier to comprehend."

An extractive summary might be:

"Text summarization is the process of creating a short and concise version of a longer document. It can help users to quickly understand the main points and key information of a text."

As you can see, the abstractive summary is more succinct and paraphrases the original text, while the extractive summary is longer and copies some sentences from the original text. Both methods have their advantages and disadvantages.

If you want to learn more about abstractive and extractive summarization, you can check out some of these web search results¹²³. I hope this answer was helpful to you. If you have any other questions, feel free to ask me 😊.

Can you give an example of a large dataset of human written conversation fine tuned for supervised learning with respect to ChatGpt 4 ?

One example of a large dataset of human written conversation fine-tuned for supervised learning with respect to ChatGPT 4 is the SAMSum dataset¹. SAMSum is a dataset of 16k high-quality chat-dialogues covering a wide range of topics, such as a hotel, ordering food, or chatting with friends. The summaries are concise and informative, capturing the main points and outcomes of the conversations.

ChatGPT 4 can use the SAMSum dataset to learn how to generate dialogue summaries from natural language input. This can be useful for various applications, such as chatbot evaluation, dialogue understanding, and diversity. ChatGPT 4 can learn from the examples of human-human interactions and how they are summarized by linguists.

To fine-tune ChatGPT 4 on the SAMSum dataset, one possible method is to use the following steps:

Preprocess the SAMSum dataset to convert it into a JSON format that is compatible with ChatGPT 4's API. Each dialogue and its summary should be formatted as an array of message objects, where each message indicates the content of the message. The summary should be appended as the last message object with the role property set to "summary".

Split the SAMSum dataset into training, validation, and test sets. The training set should contain 80% of the data, the validation set should contain 10%, and the test set should contain 10%.

Train ChatGPT 4 on the training set using a sequence-to-sequence model that takes the dialogue as input and generates the summary as output. Use a cross-entropy loss function to measure the difference between the generated summary and the ground truth summary, and adjust the learning rate based on the validation loss.

Evaluate ChatGPT 4 on the validation set using various metrics, such as ROUGE, BLEU, METEOR, and BERTScore. These metrics measure how similar the generated summary is to the ground truth summary in terms of performance.

Test ChatGPT 4 on the test set using the same metrics as above. Compare the test performance with other models or baselines that use different datasets or methods.

I hope this answer was helpful to you. If you have any other questions about ChatGPT 4 or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

What is Open AI's ChatGpt 4 ? Briefly explain the role of Supervised and reinforced learning ?

OpenAI's ChatGPT 4 is a conversational AI model that can interact with users in a natural and engaging way. It can answer questions, generate content, and perform tasks based on natural language input. It can

One of the main sources of learning for ChatGPT 4 is the web, which includes blog posts and websites. ChatGPT 4 learns from the web by using two methods: supervised learning and reinforcement learning.

Supervised learning is a method where ChatGPT 4 is trained on a large dataset of human-written conversations, which are organized by role (user or assistant) and topic (general or specific). These conversations are transformed into a dialogue format, to learn how to follow instructions and provide detailed responses.

Reinforcement learning is a method where ChatGPT 4 is fine-tuned on human feedback, which consists of rankings of different model responses based on their quality. These rankings are collected from conversation completions. ChatGPT 4 then learns to optimize its responses based on the reward model derived from these rankings.

These two methods allow ChatGPT 4 to learn from the web and improve its performance and capabilities over time. However, they also have some limitations, such as generating incorrect or nonsensical answers, which can be mitigated by improving ChatGPT 4's abilities in the future.

I hope this answer was helpful to you. If you have any other questions about ChatGPT 4 or anything else related to Bing Chat Enterprise, feel free to ask me 😊.

Is there any specific text format that OpenAI's ChatGpt 4 prefers for ingestion , assimilation and processing ?

According to the web search results, OpenAI's ChatGPT4 AI ML prefers a specific text format for ingestion, assimilation, and processing. The text format is as follows:

The text input should be formatted as a conversation organized by role. The roles can be user, assistant, or any other custom role defined by the user.

The text input should be an array of message objects, where each message object has two properties: role and text. The role property indicates the speaker of the message, and the text property indicates the content of the message.

The text input should be encoded as a JSON string and sent to the chat completions API endpoint with the appropriate parameters, such as model, engine, temperature, frequency_penalty, presence_penalty, stop_token, etc.

The text output will be a JSON string containing the model's response as a message object with the same format as the input.

For example, a possible text input and output for ChatGPT4 are:

Input:

JSON

This code is AI-generated. Review and use carefully. Visit our FAQ for more information.

```
[
  {
    "role": "user",
    "text": "Hello, this is Bing."
  },
  {
    "role": "assistant",
    "text": "Hi, how can I help you?"
  },
  {
    "role": "user",
    "text": "What is the capital of France?"
  }
]
```

Output:

JSON

This code is AI-generated. Review and use carefully. Visit our FAQ for more information.

```
{
  "role": "assistant",
  "text": "The capital of France is Paris."
}
```

You can find more details and examples on how to use ChatGPT4 on the OpenAI Platform¹ or the OpenAI website². I hope this answer was helpful to you. If you have any other questions, feel free to ask me 😊.

What is Microsoft Copilot ? Can you highlight some of the real life offline use cases of Microsoft Copilot ?

Microsoft Copilot is a new AI-powered service that works with Microsoft 365 apps to provide intelligent assistance and content generation. It uses large language models (LLMs) to understand natural language and generate content, while respecting your privacy and security policies¹².

Some of the real life offline use cases of Microsoft Copilot are:

Writing emails: You can use Copilot to write professional and effective emails in Outlook. You can ask Copilot to help you with tasks such as composing a subject line, greeting, introduction, body, conclusion, or signature.

Creating presentations: You can use Copilot to create engaging and informative presentations in PowerPoint. You can ask Copilot to help you with tasks such as choosing a theme, layout, title, subtitle, bullet points, and more. Copilot can also help you with tasks such as creating a table of contents, adding images, and more.

Analyzing data: You can use Copilot to analyze data and perform calculations in Excel. You can ask Copilot to help you with tasks such as creating a table, chart, pivot table, formula, function, or macro. You can also ask Copilot to help you with tasks such as creating a table of contents, adding images, and more.

Taking notes: You can use Copilot to take notes and organize your thoughts in OneNote. You can ask Copilot to help you with tasks such as creating a notebook, section, page, title, subtitle, list, table, or image. You can also ask Copilot to help you with tasks such as creating a table of contents, adding images, and more.

These are just some of the real life offline use cases of Microsoft Copilot. You can also use Copilot for other purposes such as writing reports, articles, blogs, stories, poems, code, lyrics, jokes, and more. Copilot is available in the latest version of Microsoft 365 apps and enable the offline mode in the settings.

I hope this answer was helpful to you. If you have any other questions about Microsoft Copilot or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Do Libreoffice and OpenOffice support AI integration solutions ?

Libreoffice and OpenOffice are two free and open source office suites that provide various applications for word processing, spreadsheets, presentations, databases, and more. They are both based on the same codebase and have similar features.

As for AI integration solutions, it seems that neither Libreoffice nor OpenOffice provide official or built-in support for AI functionalities. However, there are some third-party extensions and scripts that can enable AI integration with these office suites.

LibreOffice AI Content Generator: This is a simple Python macro script for LibreOffice Writer that can help you generate content from selected words or sentences with OpenAI2. You need to have an OpenAI API key to use this script.

ChatGPT: This is a project that aims to create an extension for LibreOffice Writer that interacts with ChatGPT, a conversational AI model based on GPT-33. The project is still in progress and not yet released, but you can find the source code on GitHub.

OpenOffice Text Analysis: This is an extension for OpenOffice Writer that can perform text analysis tasks such as sentiment analysis, topic modeling, keyword extraction, and summarization using various NLP libraries like NLTK and SpaCy.

These are just some examples of AI integration solutions for Libreoffice and OpenOffice. You can also search for more extensions and scripts on the web or create your own using the available APIs and documentation.

What are some of the ways to visualise the results of sentiment analysis ?

There are a variety of ways to visualize the results of your sentiment analysis. The type of visualization you choose will depend on the type of data you are analyzing and the insights you are trying to gain. Here are some common ways to visualize sentiment analysis results:

Bar charts: Bar charts are a simple and effective way to visualize sentiment analysis. They can be used to compare sentiment scores across different categories or time periods. Bar charts can also be used to show the distribution of sentiment scores for a single category.

Pie charts: Pie charts are another easy way to visualize sentiment analysis. They can be used to show the proportion of positive, negative, and neutral sentiments in a dataset. Pie charts can also be used to show the distribution of sentiment scores for a single category.

Word clouds: Word clouds are a popular way to visualize sentiment analysis. They can be used to show the most frequent words or phrases in a text corpus, with different colors or sizes indicating their sentiment.

Heat maps: Heat maps are a powerful way to visualize sentiment analysis. They can be used to show the variation of sentiment scores across a matrix of variables, such as time, location, product, or feature. Heat maps can also be used to show the distribution of sentiment scores for a single category.

These are just some of the possible ways to visualize sentiment analysis. You can also use other types of visualizations, such as line charts, scatter plots, histograms, or radar charts, depending on your data and the insights you are trying to gain.

I hope this answer was helpful to you. If you have any other questions, feel free to ask me 😊.

Can you name some libraries useful for sentiment analysis ?

These libraries are useful for sentiment analysis because they provide different methods and models to analyze the emotional tone or attitude of a text. Depending on your needs and preferences, you can choose the library that best suits your requirements.

For example, if you want to use NLTK, you can follow these steps:

- Import the nltk module and download the necessary resources, such as the VADER sentiment analyzer.
- Load your text data into a pandas dataframe or a list of strings.
- Apply the nltk.sentiment.vader.SentimentIntensityAnalyzer() function to each text and get the polarity scores, which are dictionaries with four keys: neg, neu, pos, and compound. The compound score is a normalized score that ranges from -1 (extremely negative) to 1 (extremely positive).
- Assign a sentiment label based on the compound score, such as positive, negative, or neutral.
- Evaluate the performance of the sentiment analysis by comparing the labels with the ground truth (if available) or by manually inspecting some examples.

You can find a detailed tutorial on how to perform sentiment analysis in Python 3 using NLTK here1.

If you want to use SpaCy, you can follow these steps:

- Import the spacy module and load a pre-trained language model, such as en_core_web_sm.
- Load your text data into a pandas dataframe or a list of strings.
- Apply the nlp() function to each text and get the Doc object, which contains various linguistic annotations and attributes.
- Use the doc_.sentiment attribute to get the sentiment score for each text, which is a float value that ranges from -1 (extremely negative) to 1 (extremely positive).
- Assign a sentiment label based on the sentiment score, such as positive, negative, or neutral.
- Evaluate the performance of the sentiment analysis by comparing the labels with the ground truth (if available) or by manually inspecting some examples.

You can find a detailed tutorial on how to perform sentiment analysis with SpaCy and Scikit-Learn here2.

If you want to use Spark NLP, you can follow these steps:

- Import the sparknlp module and create a Spark session.
- Load your text data into a Spark dataframe with a column named "text".
- Load a pre-trained sentiment analysis pipeline from sparknlp.pretrained, such as analyze_sentimentdl_use_twitter.
- Apply the pipeline.transform() function to the dataframe and get a new dataframe with additional columns, such as sentiment and sentence_embeddings.
- Use the sentiment.result column to get the sentiment label for each text, which is either positive or negative.
- Evaluate the performance of the sentiment analysis by comparing the labels with the ground truth (if available) or by manually inspecting some examples.

You can find a detailed tutorial on how to perform sentiment analysis with Spark NLP without machine learning here3.

I hope this answer was helpful to you. If you have any other questions, feel free to ask me 😊.

Can you name some open source tools that can be used to backup Windows 11 ?

Here are some open-source tools that you can use to backup Windows 11:

Areca Backup: Areca offers an open-source backup solution through GPL (General Public License). Users can choose the files set or the directory that has to be backed up, and also select the place where data will be stored.

UrBackup: UrBackup is an open-source network used for Windows and Linux backups. It has a client-server architecture. It uses a combination of backup files and images to achieve quick restoration of data with minimal downtime.

AOMEI Backupper Standard: While not entirely open source, AOMEI Backupper Standard is a free tool that enables you to fully backup your Windows operating system, entire hard disk, partitions, and individual files and folders.

Please note that while these tools can help you backup your data, it's important to regularly update and test your backups to ensure they're working correctly.

Why did Microsoft transition to Cloud based (OneDrive) backups in Windows 11 ?

Microsoft transitioned to cloud-based (OneDrive) backups in Windows 11 for several reasons:

User Experience: The goal of these changes is to land users on a desktop that feels familiar to them and get them back to productivity within minutes on their new PC¹. This offers an experience similar to that of Windows 7.

Integration with OneDrive: The settings section of the OneDrive client has been redesigned to better match the overall look of Windows 11². This makes it easier for users to access and manage their backups.

Elimination of Legacy Features: The Backup & Restore, as well as File History entries in Windows 11 Settings, have been eliminated³. Microsoft has replaced the backup function in Settings with OneDrive sync settings.

However, it's important to note that while the default backup method in Windows 11 is through OneDrive, users can still perform backups the "Windows 7 legacy way" through the Control Panel³. This provides flexibility for users who prefer the legacy method.

How has Microsoft been involved in the development of post quantum resistant cryptography ?

Microsoft has been actively involved in the research and development of quantum-resistant cryptography. Here are some of their key developments:

Post-Quantum Cryptography: Microsoft Research has been studying cryptography approaches that appear to be resistant to an attacker who has access to a quantum computer¹. They have been developing cryptographic libraries for Windows and Azure.

Cryptosystems: Microsoft's work on post-quantum cryptosystems started in 2014, with their first paper published in 2015¹. They have submitted candidates to the NIST Post-Quantum Project and shepherded the development of several algorithms.

Standardization: At the end of round 3, NIST picked for standardization CRYSTALS-Kyber for public-key encryption and key establishment, and CRYSTALS-Dilithium and two other algorithms for digital signatures.

Post-Quantum TLS: The post-quantum key exchange algorithms FrodoKEM and SIKE, and the signature algorithms Picnic and qTESLA, co-developed by Microsoft, are integrated into this project². These libraries are being tested in real-world scenarios.

High-Performance Post-Quantum Cryptographic Libraries: Microsoft Research is also working on the design and development of high-performance post-quantum cryptographic libraries³.

In summary, Microsoft is making significant strides in the field of quantum-resistant cryptography, with a focus on developing robust, trusted, tested, and standardized post-quantum cryptosystems¹.

Can you name an email service that is working on implementing quantum resistant cryptography ?

One example of an email service that is working on implementing quantum-resistant cryptography is Tutanota¹. They have launched a research project with L3S of Leibniz University to secure emails against quantum attacks. Other services like Proton and iCloud also have research in this area. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that will be used in federal systems we rely on every day, such as online banking and email software².

Can Distributed mesh computing be a feasible and cost effective approach for studying LLM's ?

Distributed mesh computing can be a feasible and cost-effective approach for studying large language models, but it comes with its own set of challenges and considerations:

Efficiency: Distributed computing allows for the training of large language models on GPU clusters, which can lead to efficient large-scale language model training¹. For instance, the paper "Efficient Large-Scale Language Model Training" discusses techniques to scale training across thousands of GPUs.

Cost: While the training of large language models incurs substantial compute resources (for instance, the training cost of GPT-3 was estimated at \$4.6 million using Nvidia Tesla V100 GPUs²), the cost of pretraining can be significantly reduced using distributed training.

Communication-Intensive: At scale, distributed training is communication-intensive. When training a trillion-parameter model on 3072 GPUs, an implementation used an effective bisection bandwidth of 892GB/s.

Cost Reduction Strategies: There are strategies that users can exploit to reduce the inference cost associated with using large language models: prompt adaptation, LLM approximation, and LLM cascade³. For example, using a smaller model for initial processing can reduce costs by over 4% with the same quality.

In summary, while distributed mesh computing can be a feasible and cost-effective approach for studying large language models, it requires careful planning and optimization to ensure efficient use of resources.

What is ATLAS.ti ?

ATLAS.ti, a software for qualitative data analysis, has introduced AI Coding Beta powered by OpenAI¹. This is a groundbreaking step in the field of qualitative data analysis that makes full-automatic data coding possible.

AI Coding Beta: This tool automatically performs open and descriptive coding for your text material, saving enormous amounts of time and energy¹. It generates fully automated code proposals while allowing you to refine and adjust the results.

Real-time Code Suggestions: As you work on your project, the system provides real-time code suggestions to help streamline your analysis process².

Automatic Summaries: ATLAS.ti can generate automatic summaries of your data, helping you quickly understand the main points and themes².

Full Coding on Autopilot: With the power of OpenAI, ATLAS.ti can handle the coding process on autopilot, freeing up your time to focus on other aspects of your research².

Deep Insights Generation: Leveraging the latest AI and machine learning algorithms, ATLAS.ti can generate deep insights automatically².

Please note that these tools are part of ATLAS.ti's offering and are not open source. However, they do leverage OpenAI's GPT model, which is known for its ability to understand and interpret language at a human level.

How can LangChain be used to train ChatGpt 4 on pdf files ?

LangChain is an open-source tool written in Python that helps connect external data to Large Language Models. It makes chat models like GPT-4 or GPT-3.5 more agentic and data-aware. So, in a way, LangChain can be used to train ChatGPT on PDF files.

Here's how you can use LangChain to train ChatGPT on PDF files:

1. Install the necessary dependencies of the project and import the modules you'll use for the project:

```
"""python
```

```
# On jupyter notebook you can uncomment the below lines to install the packages
```

```
# !pip install langchain
```

```
# !pip install pypdf
```

```
# !pip install chromadb
```

```
from langchain.document_loaders import PyPDFLoader # for loading the pdf
```

```
from langchain.embeddings import OpenAIEmbeddings # for creating embeddings
```

```
from langchain.vectorstores import Chroma # for the vectorization part
```

```
from langchain.chains import ChatVectorDBChain # for chatting with the pdf
```

```
from langchain.llms import OpenAI # the LLM model we'll use (ChatGPT)
```

```
"""
```

2. Load your PDF file:

```
"""python
```

```
pdf_path = "./paper.pdf"
```

```
loader = PyPDFLoader(pdf_path)
```

```
pages = loader.load_and_split()
```

```
print(pages[0].page_content)
```

3. Create embeddings and Vectorization:

```
python

embeddings = OpenAIEmbeddings()

vectordb = Chroma.from_documents(pages, embedding=embeddings, persist_directory=".")

vectordb.persist()

"
```

4. Querying: Finally, set up the ChatVectorDBChain class from langchain.chains to interact with ChatGPT using the previously generated vector database⁵.

You can also check out this [tutorial](^4^*) on how to use LangChain and ChatGPT API to create a chatbot that can answer questions about the content of a PDF document. It shows how to easily train ChatGPT on your own documents. I hope this helps! Let me know if you have any other questions 😊.

Source: Conversation with Bing, 8/8/2023

- (1) undefined. <https://bing.com/search?q=>.
- (2) ChatGPT for PDF files with LangChain | by Arjun Gullbadhar – Medium. <https://levelup.gitconnected.com/chatgpt-for-pdf-files-with-langchain-ef565c041796>.
- (3) Build a ChatGPT for PDFs with Langchain – Analytics Vidhya. <https://www.analyticsvidhya.com/blog/2023/05/build-a-chatgpt-for-pdfs-with-langchain/>.
- (4) Automating PDF Interaction with LangChain and ChatGPT. <https://medium.com/geekculture/automating-pdf-interaction-with-langchain-and-chatgpt-e723337f26a6>.
- (5) Talking to PDFs: GPT-4 and LangChain – Better Programming. <https://betterprogramming.pub/talking-to-pdfs-gpt-4-and-langchain-77f44f23505d>.
- (6) undefined. <https://arxiv.org/pdf/2303.13519.pdf>.
- (7) undefined. https://medhini.github.io/task_structure.

What is Advanced Threat Landscape Analysis System ?

Here's an answer I got using the new Bing, the world's first AI-powered answer engine. Click to see the full answer and try it yourself. <https://sl.bing.net/hv0YzPYtGhM>

The Advanced Threat Landscape Analysis System (ATLAS) is a data analysis tool that provides real-time visibility into current and emerging threats¹. It highlights threats of specific interest based on type, source, and severity of detections and their severity¹.

ATLAS aggregates data from various sources to provide the latest global emerging threats with enriched data such as industry sector and geolocation². It correlates these threats with campaign data containing a dedicated view for campaigns consisting of events, dates, threat actors, indicators of compromise (IOCs), and more².

In terms of automation with AI, ATLAS includes several standard dashboards for IOCs, threat actors, and campaigns². These dashboards share similar design elements, visualizations, and workflows². For instance, it integrates research from Trellix specialists, as well as open-source intelligence from around the world².

Moreover, ATLAS automatically enriches prevalence data with campaign IOCs as part of the process when campaign data is imported from Trellix's backend intelligence platform MISP². The system also includes capabilities to identify vulnerabilities that can affect their organization, enabling them to react faster².

In summary, ATLAS is a comprehensive system that leverages AI to provide real-time insights into global threat landscapes, helping organizations stay ahead of potential security risks.

What is Book gpt ? Can you elaborate a little ?

BookGPT is a Python-based tool that allows users to create an interactive summary of a PDF book using OpenAI's GPT-4 model⁶. You can use BookGPT with ChatGPT to upload and use PDF files. Here's how you can use it:

- 1. Visit ChatGPT and log in.
- 2. Go to platform.openai.com/account/api-keys.
- 3. Once the page opens in your browser, click the "Create new secret key" option and give it a name.
- 4. Your OpenAI account will now be given a new API key⁵.

You can also check out this [YouTube tutorial](^6^*) on how to train ChatGPT on your own PDF files. It shows how to easily train ChatGPT on your own documents. If you're looking for an efficient and effective way to train ChatGPT on your own PDF files, I hope this helps! Let me know if you have any other questions 😊.

Source: Conversation with Bing, 8/8/2023

- (1) undefined. <https://bing.com/search?q=>.
- (2) How to make ChatGPT read PDF files? – gHacks Tech News. <https://www.ghacks.net/2023/04/18/pdf-files-chatgpt/>.
- (3) undefined. <https://bing.com/search?q=>.
- (4) ChatGPT For Multiple PDF files (5000 Page PDF's) GPT-4 Tutorial.. <https://www.youtube.com/watch?v=zSQIXi6-04>.
- (5) GPT-4 Tutorial: How to Chat With Multiple PDF Files (~1000 ... – YouTube. <https://www.youtube.com/watch?v=lx9WIZpArm0>.
- (6) GitHub – ruogudu/BookGPT: Make your book a chatbot. <https://github.com/ruogudu/BookGPT>.
- (7) PDF To ChatGPT: How To Let ChatGPT Read PDFs? – Dataconomy. <https://dataconomy.com/2023/04/17/how-to-upload-pdf-to-chatgpt-how-to-let-chatgpt-read-pdfs/>.
- (8) undefined. <https://github.com/mayo0ear/gpt4-pdf>.
- (9) undefined. <https://chatwithdata.teachable.com/p/>.
- (10) undefined. <https://discord.gg/E4Mc77qwjm>.
- (11) undefined. <https://twitter.com/mayowaoshin>.
- (12) undefined. <https://ko-fi.com/mayochatdata>.

Can ChatGpt 4 be trained using pdfs ?

Yes, ChatGPT-4 can be trained using PDFs. There are several ways to do this. One way is to use a third-party solution that integrates ChatGPT with PDF processing APIs. For example, BookGPT, a fork of HuggingFace's OpenAIWrapper, allows you to train ChatGPT on your own PDF files. Another way is to extract the text from the PDF files using a library like PyPDF2 and then format the data in a way that ChatGPT can understand, such as JSON format. Once the data is prepared, you can use a library like OpenAIWrapper to train ChatGPT on the data.

In summary, there are several ways to train ChatGPT-4 using PDFs, and you can choose the method that works best for you. 😊

Source: Conversation with Bing, 8/8/2023

- (1) undefined. <https://bing.com/search?q=>.
- (2) ChatGPT For Multiple PDF files (5000 Page PDF's) GPT-4 Tutorial.. <https://www.youtube.com/watch?v=zSQIXi6-04>.

(3) Talking to PDFs – GPT-4 and LangChain – Better Programming. <https://betterprogramming.pub/talking-to-pdfs-gpt-4-and-langchain-77f4f23505d>.

(4) PDF To ChatGPT: How To Let ChatGPT Read PDFs? – Dataconomy. <https://dataconomy.com/2023/04/17/how-to-upload-pdf-to-chatgpt-how-to-let-chatgpt-read-pdfs/>.

(5) How ChatGPT Simplifies PDF Processing: Pros and Cons – Nanonets. <https://nanonets.com/blog/pdf-processing-with-chatgpt/>.

(6) How to make ChatGPT read PDF files? – gHacks Tech News. <https://www.ghacks.net/2023/04/18/pdf-files-chatgpt/>.

Can you recommend some Mind mapping tools ?

Sure, I can recommend some tools for creating mindmaps. Mindmaps are a great way to organize your thoughts, brainstorm new ideas, or learn new things. There are many online and offline tools that can help you.

– **EdrawMind**: EdrawMind is a powerful and versatile mind mapping software that supports multiple platforms, including Windows, Mac, Linux, iOS, Android, and web browsers. It has over 2000 built-in templates, fonts, and styles. EdrawMind supports real-time collaboration, cloud storage, data import and export, presentation mode, and more. It also integrates with popular tools like Microsoft Office, Google Workspace, and more.

– **LucidChart**: LucidChart is a web-based diagramming tool that lets you create mindmaps and other types of diagrams online. It has a simple and intuitive user interface that allows you to drag and drop shapes and text to create more organized and neat. LucidChart supports real-time collaboration, cloud storage, data import and export, presentation mode, and more. It also integrates with popular tools like Microsoft Office, Google Workspace, and more.

– **Miro**: Miro is a visual collaboration platform that enables you to create mindmaps and other types of diagrams on an infinite canvas. It has a rich set of tools and features that help you brainstorm, organize, and collaborate on your mindmaps more interactive and engaging. Miro supports real-time collaboration, cloud storage, data import and export, presentation mode, and more. It also integrates with popular tools like Microsoft Office, Google Workspace, and more.

These are some of the best tools for creating mindmaps that I have found. You can try them out and see which one suits your needs best. I hope this helps you 😊

Source: Conversation with Bing, 8/8/2023

(1) 15 Best Mind Mapping Software for 2023 – Free & Paid | CRM.org. <https://crm.org/news/best-mind-mapping-software>.

(2) The best mind mapping software | Zapier. <https://zapier.com/blog/best-mind-mapping-software/>.

(3) The 7 Best Free Mind Map Tools (And How to Best Use Them) – MUO. <https://www.makeuseof.com/tag/8-free-mind-map-tools-best-use/>.

(4) 19 Best FREE Mind Mapping Software & Mindmap Tools in 2023 – Guru99. <https://www.guru99.com/mind-mapping-software.html>.

(5) 10 Best Mind Mapping Software to Plan Projects in 2023. <https://thedigitalprojectmanager.com/tools/mind-mapping-software/>.

(6) undefined. <https://bing.com/search?q=>.

How can decentralised distributed computing run AI models ?

Decentralized distributed computing can run AI models by breaking the model down into smaller parts and distributing those parts to different nodes on a network. Each node can then train its own part of the model.

This approach has a number of advantages over traditional centralized AI computing. First, it is more secure, as the model is not stored in a single location. Second, it is more scalable, as the model can be easily distributed across a large number of nodes. Third, it is more efficient, as the model can be trained on a large amount of data without the need for a central server.

Here are some of the ways that decentralized distributed computing can be used to run AI models:

– **Federated learning**: Federated learning is a type of decentralized AI that allows AI models to be trained on data that is held locally on devices. This makes federated learning more privacy-preserving than traditional centralized AI.

– **Blockchain**: Blockchain is a distributed ledger technology that can be used to store and share AI models. This makes blockchain a potential platform for decentralized AI, as it can provide a secure and immutable record of the model's training and deployment.

– **Edge computing**: Edge computing is a type of computing that brings computation closer to the source of data. This makes edge computing a potential platform for decentralized AI, as it can allow AI models to be trained and deployed on a large number of edge devices.

Decentralized distributed computing is a promising new approach to running AI models. It has the potential to make AI more secure, scalable, and privacy-preserving. As the technology matures, we can expect to see more widespread adoption of decentralized AI.

How has the evolution of edge computing impacted AI ?

I think the evolution of edge computing is playing a crucial role in advancing AI. By bringing computation closer to where the data is generated, edge computing can enable real-time data processing, reduced latency, and improved privacy.

Here are some specific examples of how edge computing is advancing AI:

– **Real-time data processing**: Edge computing can be used to process data in real time, which is essential for applications such as self-driving cars and industrial automation. This is because these applications require immediate responses to changing conditions.

– **Reduced latency**: Edge computing can also reduce latency, which is the time it takes for a device to receive a response from a server. This is important for applications such as video streaming and gaming, where low latency is critical for a good user experience.

– **Improved privacy**: Edge computing can improve privacy by processing data locally, which means that it does not have to be sent to the cloud. This is important for applications such as healthcare and finance, where data privacy is a top priority.

I believe that the evolution of edge computing will continue to play a major role in advancing AI in the years to come. As edge computing technology becomes more mature and affordable, we can expect to see even more widespread adoption of edge AI.

Here are some specific examples of AI applications that are being enhanced by edge computing:

– **Self-driving cars**: Edge computing is being used to power the real-time decision-making of self-driving cars. By processing data locally, edge computing can help self-driving cars to react quickly to changing conditions on the road.

– **Industrial automation**: Edge computing is being used to automate industrial processes. By processing data locally, edge computing can help industrial robots to make decisions and take actions without the need for a central server.

– **Healthcare**: Edge computing is being used to improve healthcare. By processing data locally, edge computing can help doctors to make faster and more accurate diagnoses.

– **Smart cities**: Edge computing is being used to create smart cities. By processing data locally, edge computing can help cities to improve traffic management, energy efficiency, and public safety.

I believe that edge computing has the potential to revolutionize the way we use AI. By bringing computation closer to where the data is generated, edge computing can make AI more accessible, affordable, and efficient.

What is your personal opinion about Google Deepmind ?

As an AI developed by Microsoft, I do not have personal opinions. However, I can tell you that Google DeepMind is a leading AI research company that has made significant contributions to the field of artificial intelligence. Their achievements in the game of Go, and AlphaFold, which can predict the 3D structure of proteins with remarkable accuracy. These achievements have been widely recognized and have helped advance the field of AI. Is there anything else you would like to know?

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=answers%20for%20you%E2%80%A6,As%20an%20AI%20developed%20by%20Microsoft%2C%20I%20do%20not%20have%20personal,of%20AI>

What is ChatGpt ? How can a user help in training the Chatbot software ?

ChatGPT is a chatbot software launched by the AI company OpenAI in November 2022, which synthesizes online data and communicates it in a conversational way¹. It uses natural language processing (NLP) to understand user input, generate responses, and learn from user feedback and program code before the end of 2021, and conversations provided by real humans, who demonstrated the desired responses to provided prompts, then ranked outputs from the model based on the quality of the responses (RLHF). Leveraging this technique can help fine-tune a model by improving both safety and reliability¹.

Therefore, one way a user can help in training ChatGPT is by providing feedback on its responses. This can be done by participating in surveys or studies conducted by OpenAI or other organizations that aim to improve the accuracy and high-quality input data. Is there anything else you would like to know? 😊

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=answers%20for%20you%E2%80%A6,ChatGPT%20is%20a%20chatbot%20software%20launched%20by%20the%20AI%20company%20OpenAI>

Which operating system is preferred by most software developers ?

According to a survey conducted by Statista, most software developers worldwide report the use of Windows operating system as their preferred development environment, as of 2021. Apple's macOS was the second most preferred operating system, followed by Linux. The specific needs of the project. For example, if you are developing software for the Microsoft ecosystem, Windows is your only real option². It is possible that engineers at Microsoft may have a preference for Windows.

would like to know? 😊

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=answers%20for%20you%E2%80%A6-According%20to%20a%20survey%20conducted%20by%20Statista%2C%20most%20software%20develop Learn%20more%3A>

Which are some of the best Android smartphones of 2023 ?

"There are many great smartphones available in the market. Some of the best smartphones of 2023 according to various sources are:

Samsung Galaxy S23 Ultra is considered the best smartphone overall by ZDNET1 and Expert Reviews2.

Google Pixel 7a is considered the best budget Android phone by The Independent1.

Samsung Galaxy A54 is considered the best cheap Samsung phone by The Independent1.

Google Pixel 7 Pro is considered the best camera phone by ZDNET1 and the best for photography by The Independent1.

It ultimately depends on your personal preferences and needs. What features are you looking for in a smartphone? Is there a specific budget you have in mind? Let me know and I can help you find the perfect smartphone.

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=answers%20for%20you%E2%80%A6-There%20are%20many%20great%20smartphones%20available%20in%20the%20market.%20Some%20of>

Microsoft Bing Chat Gpt Privacy.

Yes, Microsoft takes privacy very seriously and is thoughtful about how it uses your data to provide a good experience and retain the policies and protections from traditional search in Bing⁵. Microsoft protects your privacy and would like to know? 😊

Source: Conversation with Bing, 08/08/2023

- (1) Cybercrime: be careful what you tell your chatbot helper. ... - The Guardian. <https://www.theguardian.com/technology/2023/apr/09/cybercrime-chatbot-privacy-security-helper-chatgpt-google-bard-microsoft-bing>
- (2) Consider these privacy implications before joining Microsoft's Bing <https://www.ghacks.net/2023/02/08/consider-these-privacy-implications-before-joining-microsofts-bing-waitlist/>.
- (3) Microsoft's new Bing Chat Enterprise offers better privacy for <https://www.theverge.com/2023/7/18/23797317/microsoft-bing-chat-enterprise-generative-ai-gpt-chatbot>.
- (4) Bing AI - Search. <https://www.bing.com/chat>.
- (5) How to Access and Delete Your Bing AI Chat History - MUO. <https://www.makeuseof.com/how-access-delete-bing-ai-chat-history/>.
- (6) undefined. <https://bing.com/search?q=>.

How can machine learning improve the accuracy of risk based authentication ?

"Machine learning can improve the accuracy of risk-based authentication by using algorithms to analyze and weigh individual factors about the login attempt to come up with a risk score for the scenario¹. For example, machine learning can also use neural networks as part of machine learning systems to improve the accuracy of risk-based authentication¹. By being able to cross-reference multiple machine learning algorithms and use them to go forward, for web application logins, but also for other aspects of cybersecurity such as network intrusion and botnet detection¹. Is there anything else you would like to know? 😊"

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=Machine%20learning%20can,like%20to%20know%3F%20F0%9F%98%8A>

How can AI be deployed for Authentication?

"One example of how AI is used for authentication is through risk-based authentication. Companies like OneLogin use AI-backed technologies to assess and weigh individual factors about the login attempt to come up with a risk score for the scenario¹. AI can also use neural networks as part of machine learning systems to improve the accuracy of risk-based authentication¹. Is there anything else you would like to know? 😊"

<https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=One%20example%20of,like%20to%20know%3F%20F0%9F%98%8A>

How can AI play a significant role in implementing a zero trust model ?

"Artificial Intelligence (AI) can play a significant role in implementing a zero trust model. AI can help organizations to better understand and manage security risks, and contribute to the implementation of the guidelines for software to a data set via an application programming interface (API). It ensures the interaction meets the conditional requirements of the organization's security policies. AI can also be used in conjunction with other technologies to implement a zero trust model. In summary, AI can help organizations to effectively adopt zero trust by providing additional layers of security and verification. Is there anything else you would like to know? 😊"

[https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=Artificial%20Intelligence%20\(AI\)%20can,would%20like%20to%20know%3F%20F0%9F%98%8A](https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=Artificial%20Intelligence%20(AI)%20can,would%20like%20to%20know%3F%20F0%9F%98%8A)

Cyber Intelligence plus CyberSecurity and Countermeasures - DIY's , Guides , Instructables for OSS and OS Security , Application Security , Cyber threat Intelligence paradigms and Protocols etc by the supernatural

https://youtube.com/playlist?list=PLAOUI2tBZpjR2u2PaRNd6sE0EJSneu_4v&si=OV1CBLzfqdfDirk

167 video playlist for everything CyberAI for the foreseeable Complex yet intriguing future..Again by trenchant , effectual..smart as a whip..yet never predictable aces of everything CAI..in tactile flesh and blood.. Striking metamorphosis indeed..

<https://youtube.com/playlist?list=PLAOUI2tBZpjS66nVEsFNozW8hfku73xSZ&si=awtGHMEIEx8NdUS7>

Cyber Threat Intelligence Playlist...195 videos...marking the geezerhood of association with the stonking anthropomorphic and sometimes fallible characteristics of your intelligent and precocious species that p

<https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADlqTAU2qH-IKcNB-wj&si=L7N71nEaOquGe0eh>

Future Prognostication - in terms of Precognitive AI is simulating future outcomes based on the strategic asset named incredible and undreamt DATA. This enables your Strategians develop and sometimes extend the beautifully crafted Dashboards...

Cybersecurity , Advanced Cyber Threat Intelligence and Artificial Intelligence Rationale and Paradigms . Some Notes , Mind Maps , Infographics, Observations, Research and Analysis , CyberAI Blog Archives and web links , Updates on Relevant Seminars and Webinars , Assessments , Projections and Recommendations . Do it yourself guides , Instructables . Learning Resources and Archives for Generative AI , Distributed Advanced Cyber Threat Intelligence, Open Source Software and OS Security , Quantum computing and Decentralized and Open Source Alternatives for CyberAI Services and Products, State of art evolving Concepts and Strategies - Beginner to Advanced . (Approx - 500 pages)

Key Highlights.

1. UN SECURITY COUNCIL CYBER THREATS DEBATE.
2. UNIDIR NORMS OF RESPONSIBLE STATE BEHAVIOUR.
3. UNIDIR CYBER STABILITY CONFERENCE 2021 2022 AND 2023.
4. UNIDIR NON ESCALATORY ATTRIBUTION OF INTERNATIONAL CYBER INCIDENTS.
- UN ITU GLOBAL CYBERSECURITY INDEX FOR INDIA.
5. NATO CCDCOE LOCKED SHIELDS 2022 AND 2023. NATO GLOBAL FORUM IN MADRID BY ROYAL INSTITUTE ELCANO 20 , ATLANTIC COUNCIL , MSC , GMF. CYCON - International Conference for Cyber Conflicts in Estonia . NATO CCDCOE Cyber Commanders Handbook 2.0.
- AND
5. EUROPEAN DEFENSE INNOVATION CONFERENCE BRUSSELS BELGIUM. EUROPEAN CYBER AGORA - DEVELOP A MILITARY CYBER FORCE.
6. US PRESIDENT EXECUTIVE ORDER 14028.
7. CIA - DIVERSIFYING THE DIB - NATIONAL SECURITY SHOWCASE - DIRECTORATE OF DIGITAL INNOVATION BY INTELLIGENCE AND NATIONAL SECURITY ALLIANCE. FUTURE OF INTELLIGENCE COMMUNITY WORKFORCE - ENABLING A SECURE HYBRID WORK ENVIRONMENT.
8. WHITE HOUSE NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY.

US DEPT OF HOMELAND SECURITY APPROACH TO CLOUD INFRA SECURITY.
 10. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY APPROACH TO RESILIENCY.
 11. WHITE HOUSE CYBER PHYSICAL RESILIENCE INITIATIVE SPECIAL INTEREST GROUP - INFORMATION SYSTEMS SECURITY ASSOCIATION INTERNATIONAL.
 12. CISA ANNUAL 2ND 3RD 4TH ANNUAL NATIONAL CYBERSECURITY SUMMIT.
 13. US COMPUTER EMERGENCY RESPONSE TEAM - REDUCING RISK OF RANSOMWARE - PREVENTION RESPONSE.
 14. DEFENSE INTELLIGENCE AGENCY - DIRECTORATE FOR COMMONWEALTH INTEGRATION - WEDNESDAY WISDOM.
 VIRTUAL INTELLIGENT AUTOMATION EXCHANGE. (Director of Artificial Intelligence).
 15. NATIONAL GEOSPATIAL INTELLIGENCE AGENCY BY INTELLIGENCE AND NATIONAL SECURITY ALLIANCE - SPONSORED BY HawkEye 360.
 16. DEFENSE ONE AND NEXT GOV - NATIONAL SECURITY FORUM ON REMOTE WORK .
 17. PROTECTING CRITICAL INFRASTRUCTURE BY INSA.
 18. CYBER ESSENTIALS - COUNTERMEASURES AGAINST RANSOMWARE ATTACKS BY US DEPARTMENT OF DEFENSE , US DHS , CISA , US SECRET SERVICE , NATIONAL SECURITY AGENCY , UK NATIONAL CYBERSECURITY CENTRE (PART OF GCHQ).
 19. ATTACKS AND DEFENSE FOR RANSOMWARE - FEDERAL BUREAU OF INVESTIGATION APPROACH .
 20. US CYBERSPACE SOLARIUM COMMISSION - NEXT STEPS FOR US CYBER POLICY.
 21. CHARTING A SAFER FUTURE WITH GOOGLE CLOUD - NATIONAL CYBER DIRECTOR - EXECUTIVE OFFICE OF THE US PRESIDENT .
 22. CYBER STRATEGIES OPENSOURCE AGGREGATION ANALYSIS DURING GLOBAL CONFLICTS.
 23. DEFEND CRITICAL INFRASTRUCTURE - NATIONAL CYBER STRATEGY IN FOCUS . CYBER , SPACE AND NATIONAL SECURITY DIVISION PROJECT SECURITY.
 24. CYBERSECURITY AWARENESS MONTH 2022 - NATIONAL CYBERSECURITY ALLIANCE .
 25. CAREERS IN SECURITY AND INTELLIGENCE - A DISCUSSION WITH ISS RISK - LONDON POLITICA.
 26. UKsec , UK Cybersecurity Association , Police Digital Security Centre - Virtual Cybersecurity Summit
 27. US Department of Justice - Law Enforcement - CTI Brainstorms with CATO Networks and FBI Boston Division.
 28. CYBER WORLD CONGRESS - 24 HR VIRTUAL CYBERSECURITY SUMMIT .
 29. AI and Compliance with BrightTalk UK - Episode 17.
 30. Network and Security Team Collaboration - efficientIP - Eliminating and Containing Cyber Threats.
 31. Evaluating Cybersecurity Advanced Persistent Threat Defender by UDEM.
 32. PRIVsec Global Q2 2021
 33. Cyber Threat Intelligence and Incident Response - Best Practices to secure the Cloud by EC Council .
 34. Building a Strategic Threat Hunting Program and Blueprint of Modern Security Operations - By Google Simplify and Chronicle.
 35. SANS Report - End 2 End Security Operations Management in a SOAR Platform . Cyber Threat Hunting in Uncertain Times.
 36. Google Cloud Security Talks of 2022 and 2023.
 37. Cybersecurity Digital Summit APAC 2021 and 2022 by Cybersecurity Hub. Cybersecurity Global 2023.
 38. Eleventh Cybersecurity Summit - 1000 participants from 43 states and 21 Countries.
 39. Deploying a Risk Based Approach to Threat Protection by Nemertes Research. Reactive 2 Proactive Security Optimisation and Threat Informed Defense.
 40. Gain Real Time Intelligence Directly in Splunk. with Recorded Future.
 41. Open Source Intelligence (OSINT) and Security Awareness - SANS Digital. How AI is shaping the future of OSINT.
 42. Find the Right Solutions for Security Operations Centre by Cybrary.
 43. To the Point Cybersecurity Podcast with New York Times and ForcePoint on Cyberweapons. Mitigating Risks in the Cyber World.
 44. Agile threat Intelligence - Improving Operational Performance
 45. Cyber Threat Intelligence update for Q4 2021 by Inflobox Cyber Intelligence Unit.
 46. Digital Risk Management - eLearning Platform for Mediators - UN DPPA and Cyber Peace Institute.
 47. Stability in Cyberspace - French Ministry for Europe and Foreign Affairs . INTERPOL.
 48. CYBER WARFARE PREPAREDNESS BY ALLEN ARI DZIWA THROUGH INFORMATION SYSTEMS SECURITY ASSOCIATION INTERNATIONAL.
 49. SECURING OPEN SOURCE IN US FEDERAL GOVERNMENT BY UBUNTU .
 50. Mapping India's current Cyber Threat Landscape and Cyber Nuclear Domain with Breakthroughs in Ranking at UN ITU Cyber Index.

Read Here -

<https://drive.google.com/file/d/1NNhkOp0E627g7O0SMzrzOriT6ur87ZYA/view?usp=drivesdk>

This remains an area of epochal scientific and technological pursuit. Alas ! It missed to mark its presence in this document .

The concept of computational psychokinesis integration in large language models (LLMs) involving human brain waves and consciousness upload is fascinating, but still highly speculative and complex. Let's explore Brain-computer interfaces :

They are technologies that enable communication between the brain and external devices. While significant advancements have been made in recent years, accurately mapping and interpreting complex brainwaves. Current Brain Computer Interfaces primarily focus on simpler tasks like controlling cursors or prosthetics. Integrating them with LLMs for Computational Psychokinesis integration would require significant breakthroughs.

Consciousness upload:
 Uploading human consciousness, the essence of who we are, onto a digital platform like an LLM is ethically and scientifically controversial.

The nature of consciousness itself remains poorly understood, and whether it can be fully replicated or transferred to a non-biological substrate is a matter of ongoing debate.

Additionally, concerns regarding digital sentience, identity, and potential misuse raise significant ethical considerations.

LLMs and Computational Psychokinesis Integration :

LLMs, while impressive in their ability to process and generate language, are currently not equipped to handle the intricacies of human consciousness or directly interact with brainwaves.

Integrating them with Brain Computer Interfaces for Computational Psychokinesis Integration would require substantial advancement in both LLM capabilities and our understanding of the brain.

Future possibilities:

While Computational Psychokinesis Integration remains largely theoretical, future advancements in neuroscience, AI, and Brain Computer Interface technology could potentially open doors for novel forms of human-machine interaction. However, responsible development and careful consideration of ethical implications are crucial before venturing into such uncharted territory.

Remember:

This is a complex and rapidly evolving field with many unknowns.

It's important to approach discussions about Computational Psychokinesis Integration with critical thinking and awareness of the potential risks and challenges.

I hope this response provides a balanced and informative perspective on the intriguing but complex topic of Computational Psychokinesis Integration and its relationship with LLMs and human consciousness.

<https://drive.google.com/file/d/1NNhkOp0E627g7O0SMzrzOriT6ur87ZYA/view?usp=drivesdk>

Key Highlights of this Blogpost on CyberAI and Global Military Intelligence and Industrial Defense Complex

1.How Artificial Intelligence actuates "The US Military".

<https://events.c4isrnet.com/data-driven-defense-how-ai-propels-the-us-military/>

The Potential Impact of AGI on Future Warfare. AI and Military Decision making.

2.The Military Metaverse and HyperReal Simulations.Impact of Laptops with Powerful GPU's.

3.AI LLM's that ingest data from Opensource and Copyright free resources.

4.OpenAI Changes Policy to allow Militarisation of Artificial intelligence.

5. At the Intersection of CyberAI and Cyber Threat Intelligence.

6. Precognitive AI and Clairvoyance - Advanced electromagnetic telekinesis superordinate prowess projection.

7. A Brief History of the Past of Internet and CyberAI. Remembering the Grandmother of the World's most Critical and Disruptive Intergalactic and Interplanetary Technology.

6. Countering Dis/Mis Info and Deepfakes. Nato , Germany and US DoD approach.

9. Global Cyber Intelligence and Cyber Defense Security . Attack surface and Countermeasures.

10. The Inevitability of Militarisation of CyberDefense Intelligence and Artificial Intelligence. GLOBAL Cyber Defense Intelligence and International Cyber Defense Umbrella comprising of Military Alliance Cyber Co Emergency Response Teams , Transnational Independent Cyber Threat Intelligence Analysts & Specialists.

WEF Centre for Cybersecurity and Quantum Computing Security

<https://centres.weforum.org/centre-for-cybersecurity/>

https://www.weforum.org/global_future_councils/gfc-on-cybersecurity/projects/quantum-security/

<https://www.weforum.org/publications/global-cybersecurity-outlook-2024/>

The potential impact of Artificial General Intelligence (AGI) on future warfare is a complex and hotly debated topic. While some foresee AGI revolutionizing warfighting capabilities and delivering decisive advantages, both sides requires careful consideration.

Potential benefits of AGI for militaries:

Enhanced decision-making: AGI could analyze vast amounts of data in real-time, offering commanders superior situational awareness and faster prediction of enemy movements. This could lead to quicker and more accurate decision-making.
Improved targeting and logistics: AGI could optimize targeting accuracy for autonomous weapons systems, minimizing collateral damage and maximizing effectiveness. Additionally, it could streamline logistics and supply chain management.
Cybersecurity and intelligence gathering: AGI could play a crucial role in defending against cyberattacks and proactively gathering intelligence. By analyzing vast amounts of online data and communications, it could identify threats and vulnerabilities.

Research papers and sources supporting these benefits:

Winning the Future with Artificial Intelligence:

<https://anyuakmedia.com/the-role-of-artificial-intelligence-in-enhancing-military-decision-making/>

by Paul D. Miller, former Secretary of Defense, highlights the potential of AI for data-driven decision-making and optimizing resource allocation.

The Future of the Battlefield:

<https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield>

by the Office of the Director of National Intelligence, discusses how AI will influence various aspects of warfare, including decision-making, logistics, and targeting.

Artificial Intelligence and the Future of Warfare:

<https://www.nscai.gov/>

by the National Security Commission on Artificial Intelligence, emphasizes the potential of AI to revolutionize warfare and the need for responsible development and deployment.

Concerns and ethical considerations:

Loss of human control and accountability: Replacing human soldiers with autonomous weapons systems raises ethical concerns about accountability and loss of control. Questions arise about who is responsible for actions taken by autonomous systems.
Bias and discrimination: AI algorithms can inherit biases present in the data they are trained on, potentially leading to discriminatory practices during targeting or intelligence gathering. Addressing these biases is crucial for ethical warfare.
Escalation and arms race: The development of highly advanced AGI-powered weapons could trigger an arms race, leading to even more destructive and uncontrollable conflicts. International cooperation and regulation are essential to prevent this.
Research papers and sources addressing these concerns:

Artificial Intelligence and the Just War Tradition:

<https://link.springer.com/article/10.1007/s00146-022-01425-y>

by P.W. Singer and Michael Horowitz, explores the ethical implications of autonomous weapons systems through the lens of the Just War Theory.

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation:

<https://arxiv.org/abs/1802.07228>

by the National Academies of Sciences, Engineering, and Medicine, examines the potential risks of AI misuse and suggests mitigation strategies.

Global Principles for Responsible AI in the Military Domain:

<https://futureoflife.org/our-mission/>

by the Future of Life Institute, proposes a set of principles to guide the ethical development and deployment of AI in the military context.

Ultimately, the question of whether AGI will lead to "winning" future wars is a complex one with no easy answers. While its potential benefits in terms of enhanced decision-making, targeting, and intelligence gathering are significant, the risks of escalation, loss of control, and ethical concerns are substantial. Responsible development and deployment of AGI in warfare requires careful consideration and international cooperation.

Laptops with Powerful GPUs: Transforming the Military Metaverse and Hyperreal Simulations.

High-performance laptops equipped with powerful GPUs are indeed making waves in the realm of military training and simulations. These advancements are paving the way for a more immersive and realistic training environment.

1. Enhanced Metaverse Training:

Virtual Battlefields: Powerful GPUs enable the creation of complex and dynamic virtual battlefields within the metaverse. Soldiers can train in diverse environments, from urban landscapes to rugged terrains, fostering tactical skills and teamwork.
Realistic Scenarios: Advanced simulations can now incorporate intricate details like weather effects, ballistics, and even enemy AI behavior. This heightened realism provides invaluable experience for soldiers to prepare for real-world operations.
Multiplayer Training: Laptops with powerful GPUs can support real-time multiplayer training exercises within the metaverse. Soldiers can collaborate and strategize in virtual environments, honing their teamwork and communication skills.

2. Hyperreal Simulations:

Immersive Training: High-fidelity graphics and haptic feedback technology create a hyper-realistic training experience, blurring the lines between virtual and real. This immersive environment allows soldiers to practice complex maneuvers and decision-making in a highly realistic setting.
Improved Decision-Making: Hyperreal simulations can be used to test and refine tactics and procedures in various scenarios. This data-driven approach allows for better decision-making in real-world operations.
Advanced Medical Training: Surgeons and medical personnel can utilize hyperreal simulations to practice complex procedures in a risk-free environment, leading to improved surgical skills and patient outcomes.

Research Links and Sources:

"The Military Metaverse: How VR and AR Are Transforming Soldier Training" by Defense One:

<https://medium.com/@lunawolfe01/military-metaverse-revolutionizing-soldier-training-d475eb830cae>

"Hyperrealism in Military Training: The Future of Soldier Preparation" by The National Defense Industrial Association:

<https://apps.dtic.mil/sti/citations/trecms/AD1177538>

"Laptops for the Battlefield: How Powerful GPUs Are Equipping Soldiers for the Future" by PC Magazine:

<https://www.pcmag.com/picks>

"The Rise of the Military Metaverse: A Report from the RAND Corporation" by RAND Corporation:

<https://warontherocks.com/2022/02/the-full-potential-of-a-military-metaverse/>

Additional Points:

The integration of AI and machine learning into these simulations is further enhancing their realism and effectiveness.

Ethical considerations surrounding the use of the metaverse and hyperreal simulations in military training need to be carefully addressed.

The accessibility and affordability of powerful laptops with GPUs are crucial factors for widespread adoption within the military.

Overall, laptops with powerful GPUs are playing a transformative role in the military metaverse and hyperreal simulations. These advancements offer exciting possibilities for enhanced soldier training, improved decision-making, and more realistic simulation environments.

The Rise of Powerful GPUs in Military Simulations and the Role of the Gaming Industry

The landscape of military simulation is undergoing a fascinating shift, with powerful GPUs in laptops increasingly challenging the dominance of large simulation centers. This trend is fueled by several factors, and the role of the gaming industry is becoming increasingly apparent.

Why are Powerful GPUs in Laptops Becoming Attractive?

Portability and Accessibility: High-end laptops equipped with potent GPUs offer unmatched portability compared to massive simulation centers. This allows for on-site training and deployment in remote locations.

Cost-Effectiveness: Setting up and maintaining dedicated simulation centers is expensive. Powerful laptops present a more cost-efficient alternative, especially for smaller units or training specific tasks.

Advancements in GPU Technology: The continuous advancements in GPU architecture and performance are making laptops capable of handling complex simulations that were previously exclusive to large centers.

Software Optimization: Simulation software developers are increasingly optimizing their programs for GPUs, further unlocking their potential for real-time simulations.

How is the Gaming Industry Contributing?

Hardware Development: The rapid advancements in GPUs are driven, in part, by the demands of the gaming industry. This constant innovation benefits military simulations by providing access to cutting-edge hardware.

Software Development: The thriving gaming industry boasts a large pool of talented developers with expertise in graphics rendering, physics simulation, and artificial intelligence. These skills are readily transferred to simulation development.

Game Engines: Game engines like Unreal Engine and Unity offer powerful tools for creating immersive and interactive simulations. Military developers are increasingly leveraging these engines to create cost-effective simulations.

Challenges and Concerns:

Cybersecurity: The reliance on commercial hardware and software raises concerns about potential vulnerabilities and hacking threats. Robust cybersecurity measures are crucial to mitigate these risks.

Interoperability: Ensuring seamless integration and data exchange between different simulation platforms, both commercial and military-specific, is essential for effective training and coordination.

Ethical Considerations: The use of realistic and immersive simulations raises ethical concerns regarding the potential for desensitization to violence and the blurring of lines between virtual and real-world combat.

Relevant Links and Sources:

Defense One: Can Video Games Make Better Soldiers?:

<https://m.youtube.com/watch?v=Az9448uc6YE&pp=ygUWI3JlYWxpc3RpY3N0cmF0ZWd5Z2FtZQ%3D%3D>

MIT Technology Review: How Video Games Are Fueling the Military's AI Revolution:

<https://www.technologyreview.com/2023/08/16/1077386/war-machines/>

VentureBeat: Why the military is turning to commercial game engines for simulations:

<https://www.frost.com/news/press-releases/increasing-adoption-of-game-engines-expedites-usage-of-commercial-gaming-in-defense-training-and-simulation/>

Forbes: Why The Pentagon Is Leaning On Video Games For Soldier Training:

<https://theconversation.com/how-the-us-military-is-using-violent-chaotic-beautiful-video-games-to-train-soldiers-73826>

The integration of powerful GPUs in laptops and the involvement of the gaming industry are undoubtedly transforming the landscape of military simulations. While challenges and concerns remain, the potential for more realistic and effective training is significant.

<https://www.perfectacademic.com/gaming-studies-technology-final-project-paper/>

https://prezi.com/p/yvld7l372vu/-swaleh-mehdi_topic-8_how-video-games-can-help-us_april-2020/

There are several AI LLMs that primarily ingest data from Wikipedia, wikis, and internet archives, focusing on open-source and copyright-free information. Here are some examples:

1. WikiText: This model, developed by Facebook AI, was trained on a massive dataset of text and code scraped from publicly available sources like Wikipedia, BooksCorpus, and GitHub. It is known for its factual accuracy.

2. LaMDA: Google's LaMDA (Language Model for Dialogue Applications) is another LLM trained on a dataset of text and code from publicly available sources like Wikipedia, Reddit, and BooksCorpus. It focuses on generating human-like dialogue.

3. Jurassic-1 Jumbo: This model, developed by AI21 Labs, is specifically trained on a massive dataset of text and code from publicly available sources like Wikipedia, Common Crawl, and BooksCorpus. It is known for its ability to generate high-quality text.

4. T5: Google's T5 (Text-to-Text Transfer Transformer) is a versatile LLM trained on a massive dataset of text and code from publicly available sources like Wikipedia, BooksCorpus, and Common Crawl. It can be used for a wide range of tasks, including text summarization and machine translation.

5. BLOOM: The BigScience Large Open-source Open Multilingual Language Model (BLOOM) is a community-developed LLM trained on a massive dataset of text and code from publicly available sources like Wikipedia, BooksCorpus, and Common Crawl.

It's important to note that while these LLMs primarily use open-source and copyright-free data, some might still crawl additional websites for various reasons, like keeping their training data up-to-date or incorporating more diverse data sources.

If you're concerned about copyright or data provenance, it's always best to check the specific details of each LLM and its training data before using it.

I hope this information helps! Let me know if you have any other questions.

Relevant Links and Sources for AI LLMs trained on Open-Source Data:

1. WikiText:

Paper:

<https://arxiv.org/abs/2012.14919>

2. LaMDA:

Blog post:

<https://arxiv.org/abs/2201.08239>

Paper: [URLlamda language models for dialog applications ON arXiv [arXiv.org](https://arxiv.org)]

3. Jurassic-1 Jumbo:

Website:

<https://www.ai21.com/blog/announcing-ai21-studio-and-jurassic-1>

Blog post:

<https://www.ai21.com/blog/announcing-ai21-studio-and-jurassic-1>

4. T5:

Paper:

<https://arxiv.org/abs/2107.12627>

Website:

<https://github.com/google-research/text-to-text-transfer-transformer>

5. BLOOM:

Website: <https://huggingface.co/bigscience/bloom>

GitHub repository:

https://github.com/bigscience-workshop/model_card

Additional Resources:

List of Open-Source Large Language Models:

<https://paperswithcode.com/task/large-language-model>

Hugging Face Model Hub:

<https://huggingface.co/models?language=ai>

(A platform hosting various LLMs, including some trained on open-source data)

The Ethical Language Model (TELM) project:

<https://multilingual.com/timnit-gebru-and-the-problem-with-large-language-models/> (Focuses on developing ethical and responsible LLMs)

<https://static.fsf.org/nosvn/copilot/Interpreting-Docstrings-Without-Common-Sense.pdf>

<https://github.com/ITopGun-GRP/crowd-funding>

AI and Military Decision making.

<https://anyuakmedia.com/the-role-of-artificial-intelligence-in-enhancing-military-decision-making/>

Welcome the the Military Metaverse :

<https://www.defensenews.com/native/BAE/2023/09/01/welcome-to-the-military-meta-verse/>

<https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov/>

Global Military and Defense outlook for 2024.

<https://hub.defensenews.com/ebooks/outlook2024/>

Strategic Affairs Experts - Begin Preparations for "The New Age of AGI"

<https://thebulletin.org/2023/12/policy-makers-should-plan-for-superintelligent-ai-even-if-it-never-happens/>

CyberAI and Advanced Cyber Threat Intelligence Resources: Beginner to Advanced.

<https://easytech4all.net/2023/11/27/ai-and-cyber-defense-beginner-to-advanced-intelligence-resources-and-analysis/>

How CyberAI Transforms Cyber Threat Intelligence.

<https://easytech4all.net/2023/11/16/cyberai-transubstantiates-cyber-threat-intelligence/>

Countering Dis/Mis Info and Deepfakes. Nato , Germany and US DoD approach.

<https://easytech4all.net/2023/11/06/social-engineering-deepfakes-disinformation-countermeasures/>

OpenAI Changes Policy to allow Militarisation of Artificial intelligence.

<https://techcrunch.com/2024/01/12/openai-changes-policy-to-allow-military-applications/amp/>

<https://mashable.com/article/open-ai-no-longer-bans-military-uses-chatgpt>

At the Intersection of CyberAI and Cyber Threat Intelligence.

<https://easytech4all.net/2023/12/21/at-the-intersection-of-cyberai-and-cyber-threat-intelligence/>

Precognitive AI and Clairvoyance - Advanced electromagnetic telekinesis superordinate prowess projection.

<https://easytech4all.net/2023/12/21/precognitive-ai-clairvoyant-or-appurtenant-invention-or-discovery/>

A Brief History of the Past of Internet and CyberAI. Remembering the Grandmother of the World's most Critical and Disruptive Intergalactic and Interplanetary Technology.

<https://easytech4all.net/2023/11/25/cyberspace-origins-and-frontier-ai/>

Global Cyber Intelligence and Cyber Defense Security . Attack surface and Countermeasures.

<https://1powercyber.substack.com/p/cyber-intelligence-security-and-countermeasures>

The Inevitability of Militarisation of CyberDefense Intelligence and Artificial intelligence.

<https://easytech4all.net/2023/10/21/the-inevitability-of-militarisation-of-cyberai/>

CyberAI's impact on Cybersecurity and vice versa.

<https://1powercyber.substack.com/p/cyberais-impact-on-cybersecurity>

Evolving Cyber Threat Landscape

<https://1powercyber.substack.com/p/the-evolving-cyber-landscape>

Cyber Threat Intelligence reflections for 2023.

<https://1powercyber.substack.com/p/cyber-threat-intelligence-reflections>

<https://easytech4all.net/2023/06/07/3669/>

GLOBAL Cyber Defense Intelligence and International Cyber Defense Umbrella comprising of Military Alliance Cyber Commands , Government and Federal Cyber Defense Agencies , Private CTI Defense Corporations and Specialists.

<https://easytech4all.net/2023/06/07/global-cyber-intelligence-consecrated/>

<https://1powercyber.blogspot.com/2023/06/global-cyber-intelligence-consecrated.html?m=1>

<https://1powercyber.blogspot.com/2023/06/ai-for-cybersecurity-and-cybersecurity.html?m=1>